OPEN ALJ

AUSTRIAN LAW JOURNAL

Ausgabe 2/2017

Schwerpunkt

Tagung
Die digitalisierte Person

AUSTRIAN LAW JOURNAL

ISSN: 2409-6911

www.austrian-law-journal.at

Editorial

Erste ALJ-Tagung: „Die digitalisierte Person“

Mit 2/2017 geht die siebte Ausgabe des Austrian Law Journal online. Der Grund, ihr ein Editorial voranzustellen, liegt darin, dass sie im Kern der ersten Tagung des ALJ gewidmet ist, die am 6. 4. 2017 an der rechtswissenschaftlichen Fakultät der Universität Graz stattfand und die „digitalisierte Person“ ins Visier nahm.

Die Digitalisierung unseres Umfeldes – man spricht bereits von digitaler Transformation der Gesellschaft – ist nicht mehr zu übersehen. Sie erfasst einzelne, private Individuen ebenso wie ArbeitnehmerInnen im beruflichen Alltag, sämtliche Gesellschaftsschichten und zunehmend alle Altersgruppen. Sie ist grenzüberschreitend ubiquitär und omnipräsent. Social Media, Internet der Dinge/Körper, Robotik, Kryptowährungen, „smarte“ Dinge und ebensolche Verträge benennen nur einige der sichtbareren Erscheinungsformen der Digitalisierung, die heute bereits Realität sind. Das ALJ, das diese Technologie als *open access* online Fachzeitschrift der Rechtswissenschaften Österreichs von Anfang an positiv nutzt, erkennt die großen Fragen, die diese Technologie gerade auch im juristischen Kontext aufwirft. Und ging ihnen in einer wissenschaftlichen Veranstaltung nach, die die Themen fokussiert auf die „Person“ aufbereitete.

Nach der Eröffnung und Begrüßung durch Univ.-Prof. Dr. *Peter Scherrer*, Vizerektor für Forschung und Nachwuchsförderung, behandelten acht RechtswissenschafterInnen im Wechselspiel von Referat und Kommentar vier zentrale Themenblöcke. Die Moderation übernahmen Univ.-Prof. Dr. *Brigitta Lurger* und Univ.-Prof Dr. *Elisabeth Staudegger*.

Zu „Digitalisierung und Selbstbestimmung“ trug Univ.-Prof. Dr. *Iris Eisenberger*, M.Sc. (LSE) von der Universität für Bodenkultur Wien vor. Univ.-Prof. Dr. *Christoph Bezemek*, B.A., LL.M. (Yale), Universität Graz, verfasste dazu einen ebenso kritischen wie lebendigen Kommentar. Danach skizzierte Assoz. Prof. Dr. *Thomas Kröll*, Wirtschaftsuniversität Wien den „digitalisierten Forscher“, den Univ.-Prof. Dr. *Stefan Storr*, Universität Graz, als langjähriger Forschungsdekan pointiert mit reicher Erfahrung aus der Praxis kommentierte. Prof. Dr. *Gregor Kirchhof*, LL.M., Universität Augsburg erkannte am Beispiel des digitalisierten Steuerzahlers die Digitalisierung als großes Potenzial für eine moderne Steuergesetzgebung und wurde von Univ.-Prof. Dr. *Tina Ehrke-Rabel*, Universität Graz, um österreichische Aspekte ergänzt. Der Nachmittag stand zunächst im Zeichen des Datenschutzes in den sozialen Medien. Prof. Dr. *Johannes Hager*, Universität München, nahm allerdings anstelle der üblichen öffentlich-rechtlichen eine privatrechtliche Perspektive ein, die Univ.-Prof. Dr. *Stefan Perner*, Universität Linz, wiederum aus österreichischer Sicht konzise variierte. Den digitalisierten Täter und mit ihm die Erscheinungsformen des Cybercrime – vom Hacken der in den Haushalten montierten *smart meter* und selbstfahrender Vehikel über „Medjacking“ bis „Ransomware“ – behandelte und veranschaulichte Univ.-Prof. Dr. *Susanne Reindl-Krauskopf*, Universität Wien, in konkreten Punkten kommentiert von Assoz. Prof. Dr. *Christian Bergauer*, Universität Graz.

Die Inhalte der einzelnen Vorträge sollen hier nicht näher beschrieben werden; sie sind im ALJ 2/2017 verschriftlicht publiziert und damit nachhaltig zugänglich.

Trotz dieser Konzentration auf die „digitale Person" wollen wir aufgrund seiner Aktualität auch in dieser Ausgabe einen weiteren, peer-reviewten Artikel veröffentlichen. Ass.-Prof. MMMag. Dr. *Philipp Anzenberger*, Universität Graz, und Ass.-Prof. *Tjaša Ivanc*, Ph.D., Universität Marburg, befassen sich in ihrem Beitrag eingehend mit der seit 18. 1. 2017 in Geltung stehenden europäischen Kontenpfändungsverordnung (VO [EU] 655/2014 des Europäischen Parlaments und des Rates vom 15. 5. 2014 zur Einführung eines Verfahrens für einen Europäischen Beschluss zur vorläufigen Kontenpfändung im Hinblick auf die Erleichterung der grenzüberschreitenden Eintreibung von Forderungen in Zivil- und Handelssachen, ABl L 189 vom 27. 6. 2014, 59) und ziehen einen Vergleich zur Brüssel Ia-VO.

Die HerausgeberInnen wünschen allen LeserInnen eine spannende, unterhaltsame und bereichernde Lektüre!

Brigitta Lurger, Elisabeth Staudegger und Stefan Storr

AUSTRIAN LAW JOURNAL

ISSN: 2409-6911

DOI: 10.25364/1.4:2017.2.1
www.austrian-law-journal.at

Provisional Account Preservation Measures in European Civil Procedure Law

A comparison between Brussels Ia and the Regulation on the European Account Preservation Order from an Austrian and a Slovenian perspective

Philipp Anzenberger[*], University of Graz
Tjaša Ivanc[**], University of Maribor

***Abstract**: With the Regulations 1215/2012 (Brussels Ia Regulation) and 655/2014 (EAPO Regulation), the European legislator has created two new and very distinct instruments to facilitate cross-border debt recovery in civil and commercial matters. While the Brussels Ia Regulation provides for an easier recognition and enforcement of national interim measures in other EU Member States, the EAPO Regulation creates a single provisional and protective measure enabling creditors to prevent the transfer or withdrawal of the debtors' assets from any bank account located in the EU.*

This paper provides a comparative analysis of these European legal instruments by evaluating the rules on preconditions, legal remedies and the different effects of national interim measures that shall be recognised and enforced within the Brussels Ia regime and the new EAPO.

***Keywords:** European Account Preservation; Brussels Ia Regulation; cross-border debt recovery; provisional and protective measures; recognition and enforcement of interim measures; effects of a European Account Preservation Order*

I. Introduction

One of the major issues regarding the European internal market is the **lack of payment discipline.** Studies show that 98 % of enterprises face payment delays from their customers.[1] While European civil procedure law entails effective instruments to produce internationally enforceable **titles in the substance of the matter,** until very recently there were no satisfactory solutions for the issuing of internationally enforceable **provisional measures.**[2] Yet, provisional measures

* *Philipp Anzenberger* is an assistant professor at the Institute of Civil Procedure and Insolvency Law, University of Graz.

** *Tjaša Ivanc* is an assistant professor for Civil Procedure Law at the Faculty of Law, University of Maribor.

1 Euler Hermes, *Credit insurance supports companies' profitable growth – An independent research study of 2000 businesses in 10 European economies* (2006), http://www.fecma.eu/media/text/UKStudyBrochureCreditIn-surance.pdf (last visited Mar. 13, 2017).

2 Friedrich L. Cranshaw, *Der europäische Beschluss zur vorläufigen Kontenpfändung*, 22 DEUTSCHE ZEITSCHRIFT FÜR WIRTSCHAFTS- UND INSOLVENZRECHT 399, 399–400 (2012); Bettina Nunner-Krautgasser, *Der geplante Rechtsakt zur europäischen Kontenpfändung, in* DIE ANERKENNUNG IM INTERNATIONALEN ZIVILPROZESSRECHT – EUROPÄISCHES VOLLSTRECKUNGSRECHT 125, 126–130 (Burkhard Hess ed., 2014); JULIA RIEBOLD, DIE EUROPÄISCHE KONTENPFÄNDUNG 395 (2014); also cf. Tanja

represent an **indispensable tool** for **preventing the transfer or withdrawal of funds** held by the debtor (especially in a bank account). Without such measures, the subsequent enforcement of the creditor's claim against the debtor in many cases becomes substantially more difficult – even more so if the debtors' funds are located in a different Member State.[3]

In recent years, however, the European legislator has taken important steps to **overcome these shortcomings.** The **recast of the Brussels I Regulation**[4] (now called Brussels Ia Regulation;[5] applicable since 10 January 2015) not only enlarges the bandwidth of enforceable **national interim measures** (even *ex parte* measures can now be enforced under certain circumstances)[6] but also facilitates the actual enforcement by abolishing the exequatur procedure.[7] On the other hand, the entirely new **European Account Preservation Order Regulation**[8] establishes a genuine European procedure for creating provisional measures enabling the creditor to obtain a European account preservation order and preventing the withdrawal or transfer of funds held by the debtor in a bank account in a Member State.[9] This new Regulation became effective on 18 January 2017 (Art. 54 EAPO Regulation).[10]

This paper provides a comparative analysis of these two new and rather distinct instruments for European creditors. Thereby it evaluates the rules on **preconditions, legal remedies** and the **different effects** of national interim measures that shall be recognised and enforced within the Brussels Ia regime and the new EAPO. The paper mainly seeks to answer the following questions:

a) How do the two Regulations differ in scope regarding provisional account preservation measures?
b) To what extent do the new Regulations provide a **surprise effect** concerning the preservation of bank accounts?
c) What are the differences in **effect** between a European Account Preservation Order and an interim measure to be enforced according to the Brussels Ia Regulation?

Domej, *Internationale Zwangsvollstreckung zwischen Territorialitätsprinzip, Gläubigerinteressen und Schuldnerschutz*, *in* DIE ANERKENNUNG IM INTERNATIONALEN ZIVILPROZESSRECHT – EUROPÄISCHES VOLLSTRECKUNGSRECHT 109, 110–115 (Burkhard Hess ed., 2014); Claudia Reith, *Wissenswertes zur Europäischen Kontenpfändungsverordnung*, 2016 ECOLEX 780, 780.

3 Nils Harbeck, *Ein Entwurf! Zum Vorschlag einer Europäischen Verordnung zur vorläufigen Kontenpfändung in grenzüberschreitenden Verfahren*, 15 ZEITSCHRIFT FÜR DAS GESAMTE INSOLVENZRECHT 805, 805 (2012); Hubertus Schumacher & Barbara Köllensperger, *Die „Europäische Kontenpfändung" und der Schutz des Unternehmens – Gibt es noch Anpassungsbedarf am Weg zum „fair trial"?* 136 JURISTISCHE BLÄTTER 413, 413 (2014).

4 Council Regulation 44/2001 of 22 December 2000 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, 2001 O.J. (L 12) 1.

5 Regulation 1215/2012 of the European Parliament and of the Council of 12 December 2012 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters (Recast), 2012 O.J. (L 351) 1.

6 Reinhold Geimer, *Das Anerkennungsregime der neuen Brüssel I-Verordnung (EU) Nr 1215/2012, in* FESTSCHRIFT FÜR HELLWIG TORGGLER 311, 328 (Hanns Fitz et al. eds., 2013).

7 REINHOLD GEIMER, INTERNATIONALES ZIVILPROZESSRECHT ¶ 3174b–3174e (7th ed. 2015).

8 Regulation 655/2014 of the European Parliament and of the Council of 15 May 2014 establishing a European Account Preservation Order Procedure to Facilitate Cross-Border Debt Recovery in Civil and Commercial Matters, 2014 O.J. (L 189) 59.

9 Tanja Domej, *Das Rechtsbehelfsverfahren bei der europäischen vorläufigen Kontenpfändung, in* FESTSCHRIFT FÜR DAPHNE-ARIANE SIMOTTA 129, 129 (Reinhold Geimer et al. eds., 2012); Nunner-Krautgasser, *supra* note 2, at 133; Reith, *supra* note 2, at 781.

10 The economic analysis of the EAPO Regulation shows that the introduction of this instrument will encourage the full use of the EU internal market, debtors' solvency, and recovery of debts. On the other hand, unjustified orders will create a number of harmful externalities to creditors, national authorities, and financial institutions; cf. Nicolas Kyriakides, *An Economic Analysis of the European Commission's Proposal for a European Account Preservation Order* (2013), available at http://www.virtusinterpress.org/IMG/pdf/10-22495_rgcv3i4art5.pdf (last visited Aug. 14, 2017).

II. Recognition and Enforcement of Interim Measures according to Brussels Ia

A. Preconditions and Legal Remedies

1. Requirements for the Recognition and Enforcement of a Provisional Measure

The recognition and enforcement of judgments issued in other Member States is regulated in Chapter III of the Brussels Ia Regulation. For the purposes of Chapter III, the term judgment includes provisional, including protective, measures ordered by a court or tribunal which, by virtue of this Regulation, has jurisdiction as to the substance of the matter. However, it does not include provisional measures ordered by a court or tribunal without the defendant being summoned to appear, unless the judgment containing the measure is served on the defendant prior to enforcement (Art. 2 point a subpara. 2 Brussels Ia Regulation). This means that – contrary to previous case law[11] on Article 32 Brussels I Regulation – there is **no** longer any **absolute requirement for a contradictory proceeding.**[12] However, the suggested[13] inclusion of provisional measures that were issued without prior service on the defendant (if the defendant has the right to subsequently challenge the measure under the national law of the Member State of origin) did not make it into the Brussels I recast.[14] Instead, if the defendant was not summoned prior to the decision making, he or she at least has to be served with the decision prior to enforcement in a different Member State. This mechanism ensures the right to a fair hearing but comes at the cost of a far lower surprise effect of the provisional measure.[15] According to Recital 33 of the Brussels Ia Regulation, however, this restriction does not preclude the recognition and enforcement of such measures under national law. Since the Brussels Ia Regulation now **explicitly regulates *ex parte* provisional measures** (Art. 2 point a subpara. 2 Brussels Ia Regulation; unlike previously Art. 32 Brussels I Regulation), some authors argue that more favourable[16] bilateral treaties are no longer applicable.[17] Others maintain that, on the basis of Recital 33 Brussels Ia Regulation, *ex parte* provisional measures can still be recognised and enforced according to domestic law.[18]

The jurisdiction regime of the Brussels Ia Regulation (as well as its precedents) applies only to **cross-border cases.**[19] With regard to **recognition and enforcement,** Articles 36 and 39 Brussels Ia Regulation clearly state that a judgment given in a Member State shall be recognised and en-

11 Case C-125/79, Denilauler v. Couchet Frères, ECLI:EU:C:1980:130.

12 Burkhard Hess, *in* EU-Zivilprozessrecht Art. 2 EuGVVO ¶ 12–13 (Peter Schlosser & Burkhard Hess eds., 4th ed. 2015); Stefan Leible, *in* 1 Europäisches Zivilprozess- und Kollisionsrecht EuZPR/EuIPR Art. 2 Brüssel Ia-VO ¶ 15 (Thomas Rauscher ed., 4th ed. 2016).

13 Cf. *Proposal for a Regulation of the European Parliament and of the Council on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial matters (Recast)*, COM (2010) 748 final (Dec. 14, 2010) Art. 2.

14 Tanja Domej, *Ein wackeliger Balanceakt – Die geplante Verordnung über die Europäische vorläufige Kontenpfändung*, 21 Zeitschrift für Europäisches Privatrecht 496, 516–517 (2013); Xandra Kramer, *Cross-Border Enforcement and the Brussels I-Bis Regulation: Towards A New Balance Between Mutual Trust and National Control over Fundamental Rights*, 60 Netherlands International Law Review 343, 362 (2013).

15 Leible, *supra* note 12, at Art. 2 Brüssel Ia-VO ¶ 15.

16 Such treaties existed, for example, between Austria and Germany, Austria and Norway or Austria and Sweden.

17 Thomas Garber, *Einstweiliger Rechtsschutz nach der neuen EuGVVO*, 12 Ecolex 1071, 1074 (2013); Georg Kodek, *in* Europäisches Gerichtsstands- und Vollstreckungsrecht – Brüssel Ia-Verordnung (EuGVVO 2012) und Übereinkommen von Lugano 2007 Art. 36 EuGVVO ¶ 20 (Dietmar Czernich et al. ed., 4th ed. 2015).

18 Martin Illmer, Arnaud Nuyts & Jonathan Fitchen, *Scope and Definitions*, *in* The Brussels I-Regulation Recast 55, 103–104 (Andrew Dickinson & Eva Lein eds., 2015).

19 Ansgar Staudinger, *in* 1 Europäisches Zivilprozess- und Kollisionsrecht EuZPR/EuIPR Einl Brüssel Ia-VO ¶ 19 (Thomas Rauscher ed., 4th ed. 2016); Georg Kodek, *in* 5/1 Kommentar zu den Zivilprozessgesetzen Art. 1 EuGVVO ¶ 18 (Hans W. Fasching & Andreas Konecny eds., 2nd ed. 2008).

forced in the other Member States without any special procedure being required.[20] Recognition and enforcement do **not require any further cross-border relation.**[21]

One of the biggest changes introduced by the Brussels I recast was the **abolition of the exequatur procedure.**[22] Thus, any judgment given in a Member State, which is enforceable in that Member State, shall be enforceable in the other Member States **without any declaration of enforceability** being required (Art. 39 Brussels Ia Regulation). Instead, for the purposes of **enforcement** in a Member State of a judgment given in another Member State ordering a **provisional measure,** the applicant only needs to provide the competent enforcement authority with the following (Art. 42 para. 2 Brussels Ia Regulation):

1. a **copy of the judgment** which satisfies the conditions necessary to establish its authenticity;
2. the **certificate issued pursuant to Art. 53,** containing a description of the measure and certifying that:
   a. the court has **jurisdiction** as to the **substance of the matter;**
   b. the judgment is **enforceable in the Member State of origin;** and
3. where the measure was ordered without the defendant being summoned to appear, proof of service of the judgment.

2. Legal Remedies

The national provisional measures that target the debtor's bank account can, of course, be contested with **national legal remedies** in the Member State of origin. Furthermore, **on the application of any interested party,** the recognition (Art. 45 para. 1 Brussels Ia Regulation) and the enforcement (Art. 46 Brussels Ia Regulation) of a judgment **shall be refused:**[23]

a. if such recognition is manifestly contrary to public policy **(*"ordre public"*)** in the Member State addressed;
b. where the judgment was given in default of appearance, if the **defendant was not served with the document which instituted the proceedings** or with an equivalent document in sufficient time and in such a way as to enable him to arrange for his defence, unless the defendant failed to commence proceedings to challenge the judgment when it was possible for him to do so;
c. if the judgment is **irreconcilable with a judgment given between the same parties** in the Member State addressed;
d. if the judgment is **irreconcilable with an earlier judgment given in another Member State** or in a third State involving the same cause of action and between the same parties, provided that the earlier judgment fulfils the conditions necessary for its recognition in the Member State addressed; or
e. if the **judgment conflicts** with:

20 Heinrich Dörner, *in* ZIVILPROZESSORDNUNG Art 39 EuGVVO ¶ 1 (Ingo Saenger ed., 7th ed. 2017).
21 Kodek, *supra* note 19, at Art. 1 EuGVVO ¶ 18.
22 Barbara Köllensperger, *Die neue Brüssel Ia-Verordnung: Änderungen bei der Anerkennung und Vollstreckung*, *in* 4 EUROPÄISCHES ZIVILVERFAHRENSRECHT IN ÖSTERREICH – DIE NEUE BRÜSSEL IA-VERORDNUNG UND WEITERE REFORMEN 37, 50 (Bernhard König & Peter G. Mayr eds., 2015); Peter Mankowski, *in* 1 EUROPÄISCHES ZIVILPROZESS- UND KOLLISIONSRECHT EUZPR/EUIPR Vorbem zu Art. 39 ff Brüssel Ia-VO ¶ 15 (Thomas Rauscher ed., 4th ed. 2016).
23 Cf. Kodek, *supra* note 17, at Art. 36 EuGVVO ¶ 6–66; Boris Schinkels, *in* ZPO KOMMENTAR Art. 45 EuGVO ¶ 1 et seq. (Hanns Prütting & Markus Gehrlein eds., 8th ed. 2016).

i. Sections 3, 4 or 5 of Chapter II where the policyholder, the insured, a beneficiary of the insurance contract, the injured party, the consumer or the employee was the defendant; or

ii. Section 6[24] of Chapter II.

Such an **application** shall be submitted to the court which the Member State concerned has communicated to the Commission pursuant to Article 75 point a Brussels Ia Regulation (Art. 47 para. 1 and Art. 45 para. 4 Brussels Ia Regulation). In **Austria,** the competent court is the respective lower regional court (*Bezirksgericht*) that is competent for the enforcement of that very judgement.[25] **Slovenia** declared the district courts (*okrožna sodišča*) to be competent to decide on an application. The application is generally carried out according to national civil procedure law (Art. 47 para. 2 Brussels Ia Regulation); however, Art. 47 para. 3 and 4 Brussels Ia Regulation contain some special provisions regarding the documents that need to be provided as well as the (general) prohibition to require the applicant to have a postal address in the Member State addressed.

B. Implementation and Effects of the Interim Measure

1. Implementation and Effects according to Brussels Ia

It is well established [26] that a foreign judgment which has been recognised (according to Art. 36 Brussels Ia Regulation or the previously applicable provisions) "*must in principle **have the same effects** in the State in which enforcement is sought as it does in the State in which the judgment was given*".[27] Any other solution would imply that a judgment could have different effects in the Member State of origin and the Member State of enforcement, thereby obstructing the free movement of judgments.[28] The free circulation of judgments, however, is one of the primary goals of the Brussels Ia Regulation,[29] and the (spatial) **extension of the effects** of the recognised decision is unanimously considered the most appropriate instrument to reach this goal.[30] The limit for the extension is the ***ordre public*** of the Member State of recognition.[31]

The Brussels Ia Regulation does not contain any specific provisions on the **implementation** of a foreign interim measure. It therefore has to be carried out in accordance with national (enforcement) law. However, it is possible for it to contain a measure or an order **unknown in the law of the Member State addressed.** In this case that measure or order shall, to the extent possible, be adapted to a measure or an order known in the law of that Member State which has equivalent effects attached to it and which pursues similar aims and interests (Art. 54 para. 1 subpara. 1 Brus-

24 This section contains rules on exclusive jurisdiction.

25 Thomas Garber, *in* INTERNATIONALES ZIVILVERFAHRENSRECHT Art. 47 EuGVVO ¶ 1 (Alfred Burgstaller et al. eds., 2015); Kodek, *supra* note 17, at Art. 47 EuGVVO ¶ 1; Köllensperger, *supra* note 22, at 58.

26 For previously dominant theories cf. Leible, *supra* note 12, at Art. 36 Brüssel Ia-VO ¶ 4.

27 Case C-145/86, *Hoffmann/Krieg,* 1988, ECLI:EU:C:1988:61; Hess, *supra* note 12, at Art. 36 EuGVVO ¶ 2–3.

28 Leible, *supra* note 12, at Art. 36 Brüssel Ia-VO ¶ 4.

29 Cf. Recitals 1, 6, 27 and 33; Dörner, *supra* note 20, at Vorbem zu Art. 36–57 EuGVVO ¶ 1.

30 THOMAS GARBER, EINSTWEILIGER RECHTSSCHUTZ NACH DER EUGVVO – DIE INTERNATIONALE ZUSTÄNDIGKEIT FÜR DIE ERLASSUNG EINSTWEILIGER MAßNAHMEN UND DEREN ANERKENNUNG UND VOLLSTRECKUNG NACH DER EUGVVO 270 (2011); Leible, *supra* note 12, at Art. 36 Brüssel Ia-VO ¶ 4; Bettina Nunner-Krautgasser, *Die Anerkennung und Vollstreckung englischer freezing injunctions in Österreich*, 58 ÖSTERREICHISCHES BANKARCHIV 794, 797 (2010).

31 Leible, *supra* note 12, at Art. 36 Brüssel Ia-VO ¶ 4.

sels Ia Regulation).[32] Yet, such an adaptation must not result in effects going beyond those provided for in the law of the Member State of origin (Art. 54 para. 1 subpara. 2 Brussels Ia Regulation).[33]

2. Austrian Provisional Measures

In Austrian civil procedure law, interim measures (*Einstweilige Verfügungen*) are set forth in §§ 378–402 of the Austrian Enforcement Code (EO[34]). § 379 EO provides for **restraining orders to secure monetary claims;** § 379 para. 3 subpara. 3 EO holds some special provisions for cases where **third-party debtors** (for example banks) are involved. Such a restraining order is enforced by issuing a so-called double order: the debtor is served a **freezing order,** whereas the third-party debtor is served an **order prohibiting payment** and any other action that might impede the successful enforcement of the affected claim.[35] The debtor as well as the third-party debtor **can, but do not need to be, heard** before the provisional measure is issued.[36] Yet, whoever was not heard before the provisional measure was issued is granted a special (but not suspensive) objection (*Widerspruch*) in order to ensure their right to be heard (§ 397 EO). The third-party prohibition has **no effect *in rem*.**[37] Hence, the creditor does not acquire a security right (with an *erga omnes* effect) regarding the affected claim. Nevertheless, according to § 385 para. 3 EO, the third-party debtor is **liable to pay damages** caused by the disregard of the prohibition.

3. Slovenian Provisional Measures

In Slovenia, an **interim order** may be issued before any judicial procedure, during the procedure, as well as after the procedure, until the enforcement is carried out. Unlike with respect to preliminary measures, the court is free to issue, on the proposal of the creditor, any kind of interim measure. Although the law explicitly identifies only a few possible types of interim injunctions, the court may issue any order proposed by the creditor which could achieve the purpose of such preservation (Art. 271 of the Civil Claim Act (ZIZ[38])). The interim measure instructs the bank to refuse payment from the debtor's account to the debtor or another person on the debtor's instructions of the sum of money on which the interim order has been placed (Art. 271 para. 1 point 4. ZIZ). The bank may freeze the amount of money ordered in the court decree or transfer the money to a special bank account.[39] If the bank violates the prohibition to dispose of the money, it may be held liable for damages.

In Slovenia, a court's decree of interim order – if issued in a civil or any other proceeding – has the **effect of an enforcement decree** (Art. 286 ZIZ); however, it can only interfere with the sphere of the debtor but not of third parties.[40] For example, the issuing of an interim measure

32 Cf. Dörner, *supra* note 20, at Art. 54 EuGVVO ¶ 1; Leible, *supra* note 12, at Art. 54 Brüssel Ia-VO ¶ 7.
33 Dörner, *supra* note 20, at Art. 54 EuGVVO ¶ 2.
34 "Exekutionsordnung".
35 Hansjörg Sailer, *in* EXEKUTIONSORDNUNG – KOMMENTAR § 379 EO ¶ 23 (Alfred Burgstaller & Astrid Deixler-Hübner eds., 2016).
36 MATTHIAS NEUMAYR & BETTINA NUNNER-KRAUTGASSER, EXEKUTIONSRECHT 304–305 (3rd ed. 2011); WALTER RECHBERGER & PAUL OBERHAMMER, EXEKUTIONSRECHT ¶ 521 (5th ed. 2009), 521.
37 Neumayr & Nunner-Krautgasser, *supra* note 35, at 293; Rechberger & Oberhammer, *supra* note 35, at ¶ 482; Sailer, *supra* note 34, at § 379 EO ¶ 24; also cf. Erich Kodek, in KOMMENTAR ZUR EXEKUTIONSORDNUNG § 379 EO ¶ 14 (Peter Angst & Paul Oberhammer eds. 2015).
38 "Zakon o izvršbi in zavarovanju".
39 NEŽA POGORELČNIK VOGRINC, ZAČASNE ODREDBE V CIVILNIH SODNIH POSTOPKIH 251 (2015).
40 VESNA RIJAVEC, CIVILNO IZVRŠILNO PRAVO 272 (2003).

does not lead to a registered charge on the subject of insurance. Therefore, an interim order prohibiting the disposal of the subject of preservation does not prevent legal interventions of other parties in the same subject (e.g. proceedings of enforcement). As a **consequence of the debtor's violation** of such an order, the creditor therefore may challenge detrimental dispositions only in accordance with law of obligations.[41]

III. The European Account Preservation Order

A. Preconditions, Procedural Aspects and Legal Remedies

1. Requirements for the Issuing of an EAPO

The European Account Preservation Order (EAPO) is a **genuine European interim measure** aiming at facilitating the recovery of cross-border claims for citizens, seeking to preserve funds and recover bad debts.[42] It is available for pecuniary claims, if the case concerns a civil and commercial matter (Art. 2 para. 1 EAPO Regulation). **"Claims"** are defined as claims for payment of a specific amount of money that have fallen due or claims for payment of a determinable amount of money arising from a transaction or an event that has already occurred (Art. 4 para. 5 EAPO Regulation). Recital 12 explains that those claims include claims in "tort, delict and quasi-delict"; the Regulation therefore applies to most civil monetary claims.[43]

The EAPO is only available in **cross-border cases** (Art. 2 para. 1 EAPO Regulation). A cross-border case is one in which the bank account or accounts to be preserved by the Preservation Order are maintained in a Member State other than:

- the Member State of the court seized with the application for the Preservation Order pursuant to Article 6 (Art. 3 para. 1 point a EAPO Regulation),
- or the Member State in which the creditor is domiciled (Art. 3 para. 1 point b EAPO Regulation).

Since only one of the above requirements needs to be met in order to constitute a cross-border case, the only "intra-European" constellation in which the Regulation does not apply is where the **creditor's domicile, the seized court and the bank account to be preserved** are situated in the same Member State.[44] However, the Austrian legislator created a special provision making the rules of the Regulation also applicable in cases where all of the above elements are located in Austria (cf. § 422 para. 3 EO).[45]

The EAPO is available **before** the initiation of proceedings on the substance of the matter, **during** such proceedings until the judgment is adopted, **and even after** a judgment against the debtor

41 Vesna Rijavec, *Cross-border effects of provisional measures in civil and commercial matters*, *in* CROSS-BORDER CIVIL PROCEEDINGS IN THE EU 79, 91 (Vesna Rijavec & Tjaša Ivanc eds. 2012).

42 Reith, *supra* note 2, at 781. In 2004, Hess conducted a study analysing how the transparency of a debtor's assets, the attachment of bank accounts, provisional enforcement, and protective measures contributed to the enforcement of a judgment. In this study, Hess introduces the idea of a European Protective Order for cross-border garnishment of bank accounts which could supplement the legal protection of creditors provided by the Brussels Regulation. BURKHARD HESS, STUDY NO. JAI/A3/2002/02 ON MAKING MORE EFFICIENT THE ENFORCEMENT OF JUDICIAL DECISIONS WITHIN THE EUROPEAN UNION: TRANSPARENCY OF DEBTORS ASSETS – ATTACHMENT OF BANK ACCOUNTS – PROVISIONAL ENFORCEMENT AND PROTECTIVE MEASURES (2004), *available at* http://ec.europa.eu/civiljustice/publications/docs/enforcement_judicial_decisions_180204_en.pdf (last visited last visited Mar. 13, 2017).

43 FRANZ MOHR, DIE VORLÄUFIGE KONTENPFÄNDUNG ¶ 18–43 (2014).

44 Mohr, *supra* note 43, at ¶ 48.

45 More extensively on this topic Nina Martin, *Die europäische und die österreichische vorläufige Kontenpfändung*, 3 JURISTISCHE AUSBILDUNG UND PRAXISVORBEREITUNG 163, 166–167 (2016/2017).

is obtained (Art. 5 EAPO Regulation). In order to apply for a Preservation Order, the creditor uses a standard form and provides the information requested in Art. 8 EAPO Regulation. The procedure is generally written and based on the information and evidence provided by the creditor (Art. 9 EAPO Regulation). The **debtor shall not be notified** of the application for a Preservation Order or be heard prior to the issuing of the Order (*ex parte* procedure; Art. 11 EAPO Regulation).

An EAPO may be issued when two conditions are present: first, an **urgent need for an EAPO,** because there is a **real risk** that, without such a measure, the subsequent enforcement of the creditor's claim against the debtor will be impeded or made substantially more difficult (Art. 7 para. 1 EAPO Regulation);[46] second, the creditor's **likeliness to succeed on the substance of his claim** against the debtor. However, the second requirement only needs to be fulfilled if the creditor has not yet obtained, in a Member State, a judgment, court settlement or authentic instrument requiring the debtor to pay the creditor's claim (Art. 7 para. 2 EAPO Regulation).

2. Procedural Aspects

Chapter 2 governs the entire procedure for issuing an EAPO; this paper, however, seeks to highlight only two procedural points that are of interest for our comparison. One is that the **debtor shall not be notified** of the application for a Preservation Order or be heard prior to the issuing of the Order (Art. 11 EAPO Regulation). This shall ensure the **surprise effect** of the Preservation Order, helping to make it a useful tool for a creditor trying to recover debts from a debtor in cross-border cases (Recital 15 EAPO Regulation).

Moreover, in accordance with the recent developments in European civil procedure law, the EAPO shall be **recognised** in other Member States without any special procedure being required and is **enforceable** without a declaration of enforceability (Art. 22 EAPO Regulation). In return for these benefits to the creditor, the EAPO Regulation includes a number of safeguards for the debtor, such as the obligation of a creditor to provide security (Art. 12 EAPO Regulation), a creditor's liability for damage (Art. 13 EAPO Regulation), and numerous remedies against the EAPO.

3. Legal Remedies

Art. 32–39 of the EAPO Regulation contain a rather **complex system of legal remedies.**[47] Some legal remedies are available to the **creditor only** (Art. 35 para. 4 EAPO Regulation); some apply **only to the debtor** in the Member State of origin (Art. 33 EAPO Regulation) or in the Member State of enforcement (Art. 34 EAPO Regulation), whereas some can be invoked by **both the debtor and the creditor** (Art. 35 para. 1 and 3 EAPO Regulation). The procedure for these remedies is laid down in Article 36 EAPO Regulation. Seeking to compare the Brussels Ia Regulation and the EAPO Regulation, the legal remedies **provided for the debtor in the Member State of enforcement** are highlighted below.

---

46 As the Regulation does not detail how "urgent need" and "real risk" should be proved by a creditor and measured by a court, there is a concern that different interpretations of these prerequisite standards will arise throughout the EU Member States; cf. Mirela Župan, *Cross-border recovery of maintenance taking account of the new European Account Preservation Order (EAPO)*, 16 ERA FORUM 163, 172 (2015).

47 For an overview cf. Cranshaw, *supra* note 2, at 409–410; Domej, *supra* note 9, at 130–132; Mohr, *supra* note 43, at ¶ 361–448.

When the debtor files an **application** to the competent court or enforcement authority in the Member State of enforcement, the enforcement of the EAPO shall be (Art. 34 EAPO Regulation):

a. **limited** on the grounds that certain amounts held in the account should be exempt from seizure in accordance with Art. 31 para. 3 EAPO Regulation, or that amounts exempt from seizure have not, or not correctly, been taken into account in accordance with Art. 31 para. 2 EAPO Regulation (para. 1 point a).
b. **terminated** on the grounds that:
   i. the account preserved is **excluded from the scope** of the Regulation pursuant to Art. 2 para. 3 and 4 EAPO Regulation (para. 1 point b subpoint i);
   ii. the **enforcement** of the enforcement title which the creditor was seeking to secure by means of the EAPO has been **refused** in the Member State of enforcement (para. 1 point b subpoint ii) or its enforceability has been **suspended** in the Member State of origin (para. 1 point b subpoint iii);
   iii. Art. 33 para. 1 points b, c, d, e, f or g EAPO Regulation apply (in that case Art. 33 para. 3, 4 and 5 apply as well). Hence, **many** of the **grounds for a revocation or modification** of the EAPO **in the Member State of origin** (for example if there was a flaw in the service or translation of relevant documents; points b and c can also be raised as grounds for the termination of enforcement in the Member State of enforcement;[48]
   iv. it is manifestly **contrary to the public policy (*ordre public*)** of the Member State of enforcement (para. 2).

Either party has the **right to appeal** against the decision of the court (Art. 37 EAPO Regulation). Also, upon application by the debtor the competent court or authority of the Member State of enforcement **may terminate the enforcement** of the EAPO if the debtor **provides security** (or an alternative assurance in a form acceptable under the law of the Member State of enforcement) in the amount preserved in that Member State (Art. 38 para. 1 point b EAPO Regulation).

B. Implementation and Effects of the European Account Preservation Order

1. Implementation of the EAPO

The rules for the **implementation** of the EAPO are laid down in Art. 24 EAPO Regulation. According to Art. 24 para. 2, a bank that was served an EAPO shall ensure that the amounts specified in this order (with the exception of the amounts stated in Art. 31 EAPO-Regulation) are **preserved.** The bank can do so:

- by **ensuring** that that **amount is not transferred or withdrawn** from the account or accounts indicated in the order or identified pursuant to para. 4 (point a);[49] or
- where national law so provides, by **transferring** that amount to an **account dedicated for preservation purposes** (point b).

48 Martin Trenker, *Vorläufige Kontenpfändung: Überblick und ausgewählte Rechtsfragen*, *in* 4 Europäisches Zivilverfahrensrecht in Österreich – Die neue Brüssel Ia-Verordnung und weitere Reformen 129, 149 (Bernhard König & Peter G. Mayr eds., 2015).

49 Indeed, in practice, claimants regard bank accounts as priority targets for blocking debtors' assets. When this measure is in effect, it represents a delicate situation for the debtor whose funds in the bank account are important mainly for his or her daily living or business purposes. Nicolas Kyriakides, A European-Wide Preservation Order: How the Common Law Practice Can Contribute (2014), *available at* https://www.harriskyriakides.law/assets/pdf_files/EAPO-EUArticle.pdf (last visited Aug. 14, 2017).

An **account according to point b** could be held by either the competent enforcement authority, the court, the bank with which the debtor holds his or her account or a bank designated as a coordinating entity for the preservation in a given case (Recital 26 EAPO Regulation). Austrian civil procedure law, however, does not provide for an account dedicated for preservation purposes; the Austrian bank therefore has to implement the EAPO according to Art. 24 para. 2 point a EAPO Regulation.[50] In Slovenia, a bank may transfer the amount to a special account for preservation purposes indicated in the EAPO.[51]

If the EAPO was implemented according to Art. 24 para. 2 point a EAPO Regulation, upon the **request** of the debtor, the **bank is authorised to release funds** preserved and **transfer them to the account of the creditor** for the purposes of paying the creditor's claim (Art. 24 para. 3 EAPO Regulation). However, in such a case three cumulative conditions need to be met:

1. such authorisation of the bank is specifically indicated in the order according to point j of Art. 19 para. 2 (point a of Art. 24 para. 3 EAPO Regulation);
2. the law of the Member State of enforcement allows for such release and transfer (point b of Art. 24 para. 3 EAPO Regulation); and
3. there are no competing orders with regard to the account concerned (point c of Art. 24 para. 3 EAPO Regulation).

Austrian civil procedure law entails no special provision reflecting Art. 24 para. 3 point b EAPO Regulation. However, there is **no rule opposing such a fund release;** it is therefore considered admissible if the creditor explicitly requests so in the application.[52]

Subject to the provisions of Chapter 3 of the Regulation, the EAPO shall be **enforced in accordance with the procedures** applicable to the enforcement of equivalent national orders **in the Member State of enforcement** (Art. 23 para. 1 EAPO Regulation). This subsidiary application of national provisions reflects an attempt to **build on the methods and structures already in place** for the enforcement and implementation of equivalent national orders in the Member State of enforcement (Recital 23 EAPO Regulation). In **Austrian law,** the relevant provisions relating to the interim measures are laid down in §§ 378–402 EO.[53] In Slovenia, equivalent orders are interim measures under the Slovenian enforcement law (Art. 266–279 ZIZ).[54]

2. Effects of the EAPO

Evidently, one of the main effects of the EAPO is that it permits the bank to act according to the EAPO, while also making it **liable** for failure to comply with its obligations under the EAPO Regulation. This liability, however, is governed by the national law of the Member State of enforcement (Art. 26 EAPO Regulation), thus the consequences for a disregard of the EAPO can vary amongst the Member States.

50 Mohr, *supra* note 43, at ¶ 301.
51 Pogorelčnik Vogrinc, *supra* note 39, at 251.
52 Mohr, *supra* note 43, at ¶ 314.
53 *Id*., at ¶ 291.
54 There is a new amendment of enforcement law (amendment ZIZ-L) in the legislative procedure which explicitly states that for the procedure according to the EAPO Regulation, the provisions on interim measures shall be applied.

Additionally, an EAPO can have an effect on other creditors: Art. 32 EAPO Regulation states that an EAPO **shall have the same rank, if any, as an equivalent national order in the Member State of enforcement** (Art. 32 EAPO Regulation).[55] Pursuant to Recital 28 of the Regulation, if under national law certain enforcement measures have **priority over preservation measures,** the same priority should be given to them in relation to preservation orders. Furthermore, Recital 28 states that **if there are national *in personam* orders,** those orders should be considered as the "equivalent national order" for the purpose of this Regulation. Art. 32 EAPO Regulation therefore ensures that the EAPO fits into the national system of provisional measures and enforcement law by determining what other national (or even foreign, such as the interim measures that fall within the Brussels Ia regime) provisional measures, enforcement acts or even contractual obligations have priority over the EAPO. As a result, the EAPO has a very similar effect for the **debtor** and the **bank** in every Member State, whereas the effect (the rank) for **third persons** largely depends on the rank of the instruments provided by national law. For the purpose of transparency, the Member States shall communicate to the Commission whether any ranking is conferred on equivalent national orders under national law (Art. 50 para. 1 point k EAPO Regulation).

There was a debate in **Austrian literature** on whether an "equivalent national order" should be understood as an interim measure (*Einstweilige Verfügung* under § 379 EO) or a security enforcement (*Exekution zur Sicherstellung* under §§ 370–377 EO).[56] The distinction is particularly important in this case, because an interim measure does not have an *in rem* effect, whereas a security enforcement creates an actual lien (granting an *in rem* effect), giving it priority over subsequent enforcement acts from other creditors. The Austrian legislature reacted by creating an explicit provision in § 422 EO which stipulates that the **rules on interim measures shall generally be applicable** where the EAPO Regulation contains no deviating provisions (§ 422 para. 1 EO). However, where the EAPO is issued **after** the creditor has obtained a judgment, court settlement or authentic instrument, the service on the bank **shall create an executive lien** (§ 422 para. 2 EO).

In **Slovenia,** the legislature appears to follow the Austrian example. Under the proposed amendment of the Slovenian enforcement law, the rules on interim measures will apply unless the EAPO Regulation or national provisions, in the chapter that implements the regulation, provide otherwise. Where the EAPO is **issued after the creditor has obtained a court decision** or the decision of another authority which is not yet enforceable, the rules on the preliminary measure (*predhodna odredba*) will be applicable. A court may specify attachment of a sum of money to the debtor's account at the bank (Art. 260 para. 1 point 4 ZIZ). Also, as a precautionary measure, the ZIZ allows securing by establishing a lien on the collateral object.[57] If the EAPO is issued **before the creditor has obtained a court decision** (Art. 267 ZIZ), the provisions on the interim measure (*začasna odredba*) shall be applicable. However, the interim measure does not give basis for the establishment of a lien or the right to a priority for the creditor. A court's decree blocking funds can **only interfere with the sphere of the debtor.** As soon as it comes into effect, the bank cannot legally fulfil any obligations to the debtor (Art. 271 para. 1 point 4 ZIZ) and

55 In the Proposal for a Regulation Creating a European Account Preservation Order to facilitate cross-border debt recovery in civil and commercial matters this regulation was proposed with slightly different text, i.e. "The EAPO confers the same rank as an instrument with equivalent effect under the law of the Member State **where the bank account is located**".

56 Mohr, *supra* note 43, at ¶ 311–312; Trenker, *supra* note 48, at 151–152.

57 Vesna Rijavec, *Začasne odredbe v arbitražnem postopku*, 1 SLOVENSKA ARBITRAŽNA PRAKSA 9, 12 (2012), available at http://www.sloarbitration.eu/Portals/0/Prispevki/revijSA_2012_01_Rijavec.pdf (last visited Mar. 13, 2017).

can be held liable for paying compensation to the creditor. The preserved amount remains frozen until the bank receives the decision on its termination. Until then, the amount preserved is secured either by freezing the debtor's account or transferring this amount to a special account. However, the effect of freezing the debtor's account **does not necessarily provide complete protection** for the creditor. The funds may be transferred in an enforcement procedure where another creditor requires repayment of the claim from the debtor's assets. The issuing of an interim order to freeze the debtor's account does not, therefore, result in the formation of a lien on the subject of the insurance. If the conditions for the preliminary measure are met, the creditor may not apply for interim measures. However, the preliminary measure must achieve the same purpose in securing the claim as the interim measure (Art. 269 ZIZ). The preliminary measure according to the Slovenian law may be compared with the Austrian *Exekution zur Sicherstellung*, which means that the EAPO will have priority over subsequent enforcement acts from other creditors.

IV. Comparison of the Legal Instruments – Discussion

The following section seeks to highlight some of the **most important differences** between the Brussels Ia Regulation and the EAPO Regulation regarding effective account preservation in other European Member States. Evidently, the key distinction is that the Brussels Ia Regulation only regulates the **recognition and enforcement** of national (for our purpose: preliminary) titles, whereas the EAPO Regulation creates a **genuine European interim measure.** However, there are also several other, slightly more subtle divergences between these two instruments that are worth noting.

The first point of interest relates to the **different scopes** of the two regulations. As far as **recognition and enforcement** go, both regulations – in their respective Chapter III – enable the free movement of provisional account preservation measures by generally granting enforceability to national measures (Art. 39 Brussels Ia Regulation) and to an EAPO (Art. 22 EAPO Regulation) without the need for a prior declaration of enforceability. As far as the **issuing of the actual provisional measure** is concerned, Chapter II of the Brussels Ia Regulation "only" contains rules on international (and in some parts territorial) jurisdiction, while Chapter 2 of the EAPO Regulation provides for an entire and genuine procedure on the issuing of a European Account Preservation Order. The divergent conceptions of what is to be regarded a **"cross-border case",** the different **regimes of jurisdiction** as well as disparities in the **requirements for recognition and enforcement,** however, lead to a rather complex pattern of applicability of the two Regulations, as it shall be shown in the following example:

Example

A Slovenian creditor is suing an Austrian debtor at an Austrian court. He applies for an EAPO at this court according to Art. 6 EAPO Regulation. The requirement of a cross-border case is fulfilled if the creditor seeks to freeze a bank account in **Slovenia** (Art. 3 para. 1 point a EAPO Regulation) or in **Austria** (Art. 3 para. 1 point b EAPO Regulation) as well as in any other Member State (with the exception of the United Kingdom (Recital 50 EAPO Regulation) and Denmark (Recital 51 EAPO Regulation)). If the creditor seeks to freeze a bank account in **Austria,** he can also use the interim measures available in Austrian civil procedure law for this purpose (since the international jurisdiction for preliminary measures is automatically given when there is international

jurisdiction in the substance of the matter[58]). A Slovenian interim measure (or an interim measure originating from another Member State), however, would not be recognised, since the issuing court did not have jurisdiction as to the substance of the matter (cf. Art. 2 point a subpoint 2 Brussels Ia Regulation). If the creditor wishes to freeze an account in **Slovenia,** he can – apart from an EAPO – also apply for an interim measure in a Slovenian court according to Slovenian law (Art. 35 Brussels Ia Regulation), or he can apply for an interim measure in Austria and enforce it in Slovenia if the requirements of Art. 42 para. 2 Brussels Ia Regulation are met.

While *ex parte* interim measures are now considered judgments according to Article 2 point 1 subpara. 2 Brussels Ia Regulation, they have to be **served on the defendant prior to the enforcement** of the measure,[59] thereby diminishing the effectiveness of the interim measure.[60] The EAPO, on the contrary, shall in any case be issued **without prior hearing** of the defendant (Art. 11 EAPO Regulation) in order to guarantee a surprise effect (Recital 15 EAPO Regulation). Therefore, if the creditor deems the surprise effect necessary to prevent the disappearance of the debtor's assets, the EAPO will in many cases constitute a **more efficient instrument** to reach this goal.[61]

Another important difference between the respective interim measures relates to their **implementation and effects.** The **implementation** of an EAPO is largely regulated in Chapter 3 of the EAPO Regulation; national law shall only apply subsidiarily (Art. 23 para. 1 EAPO Regulation). The implementation of an interim measure to be enforced according to the Brussels Ia Regulation, on the other hand, is governed purely by national law, as long as the latter guarantees that the measure has the same effects as in the Member State of origin. The **effects** of an EAPO are partly regulated in the EAPO Regulation; the rank of the EAPO, however, is determined by the rank of the closest national instrument in the **Member State of enforcement** (Art. 32 EAPO Regulation). In contrast, the effects of an interim measure to be enforced under the Brussels Ia Regulation are **mostly determined by the law of the Member State of origin,** although slight adaptations to the legal system of the Member State of enforcement are possible, if necessary (Art. 54 para. 1 Brussels Ia Regulation). This demonstrates that the appropriate choice of instruments can have a **significant impact** on the effects of the interim measure sought by the creditor. In practice, however, the debtor will often be less informed about the legal situation of the Member State of enforcement than about the one in the Member State of origin. This might make national interim measures appear more attractive than they actually are in comparison to an EAPO.

The last difference we seek to address relates to the respective **legal remedies in the Member State of enforcement.** According to both Regulations, the violation of the *ordre public* in the Member State of enforcement as well as irregularities in the serving on the debtor constitute grounds for a legal remedy. Moreover, the Brussels Ia Regulation contains only two additional grounds for refusal of recognition and enforcement: incompatibility with a previous judgment as well as the violation of special provisions on the jurisdiction (Art. 45 para. 1 Brussels Ia Regulation). The EAPO Regulation – as a compensation for the surprise effect of the EAPO – provides several more grounds for terminating, as well as for limiting, the account preservation (Art. 34 EAPO Regulation), including the majority of grounds for revoking it in the Member state of origin

58 Cf. Garber, *supra* note 30, at 73; Leible, *supra* note 12, at Art. 35 Brüssel Ia-VO ¶ 2.

59 Franz Mohr, *Neues im internationalen Exekutionsrecht – die Neufassung der EuGVVO (Brüssel-I VO)*, 2013 DER ÖSTERREICHISCHE RECHTSPFLEGER 32, 35.

60 Garber, *supra* note 17, at 1074.

61 Cf. Domej, *supra* note 14, at 516; Martin, *supra* note 45, at 167.

(Art. 34 para. 1 point b subpoint iv EAPO Regulation). Challenging a "foreign" interim measure (to be enforced according to the Brussels Ia Regulation) is thus **significantly more difficult** than contesting an EAPO in the Member State of enforcement.

V. Conclusion

The **efficiency** of legal interim measures for cross-border debt recovery[62] in civil and commercial matters across Europe **was significantly increased** with the Brussels I recast and the EAPO Regulation. In particular, the new grounds for enforcing *ex parte* interim measures grant the creditor a certain **surprise effect** and thus provide a realistic chance to prevent the withdrawal or transfer of funds held by the debtor. The **effects** of an interim measure to be enforced within the Brussels Ia regime are mostly determined by the law of the Member State of origin, whereas the effects of an EAPO at least partly depend on the legal situation of the Member State of enforcement. The choice of the most suitable way to freeze the debtor's bank accounts will therefore significantly vary from case to case.

62 There has been concern regarding cross-border recovery of debt collection shown in the professional environment; cf. Vesna Rijavec, Jorg Sladič & José Caramelo Gomes, *Introductory chapter*, *in* SIMPLIFICATION OF DEBT COLLECTION IN THE EU 1, 1 et seq. (Vesna Rijavec, Tjaša Ivanc & Tomaž Keresteš eds., 2014).

AUSTRIAN LAW JOURNAL

ISSN: 2409-6911

DOI: 10.25364/1.4:2017.2.2
www.austrian-law-journal.at

Der digitalisierte Forscher

Thomas Kröll[*], Wirtschaftsuniversität Wien

***Kurztext**: Im 21. Jahrhundert ist der akademische Forscher nicht nur zunehmend digital informiert; die gesetzlich gebotene Evaluierung seiner Forschungsleistungen ist mitunter auch eine digital abgestützte. Dies bedeutet nicht nur Vorteile, sondern auch Risiken für den akademischen Forscher.*

***Schlagworte:** Digitalisierung, Evaluierung, fachwissenschaftsadäquate äußere Organisation wissenschaftlicher Forschung, Forschung, Informationsfreiheit, Wissenschaftsfreiheit*

I. Wissenschaftsfreiheit als Ausgangspunkt

Die von der Märzrevolution des Jahres 1848[1] entfesselten Stürme fegten nicht nur den *Metternich'*schen Polizeistaat mit all seinem Geisteszwang und seiner Bevormundung hinweg, sondern brachten auch dem akademischen Forscher in Österreich die ersehnte Freiheit. Sie befreiten ihn aus dem Prokrustesbett der Karlsbader Beschlüsse,[2] von den Maßregeln des Bundes-Universitätsgesetzes,[3] denen zufolge *„[n]iemand lehren [sollte], was die Wissenschaft für wahr und gut erkannt, was die Wissenschaft erforscht, was ihr für's Volk heilsam und ersprießlich schien*".[4] Vielmehr schrieb man *„von oben her […] Maß und Ziel der Erkenntniß des Geistes und der Wissenschaft vor, setzte in einem den Regierungsherrn beliebten und ihre Zwecke fördernden Sinn die Lehrbücher fest und entfernte die Lehrer, die dem Polizeistaat nicht mit Verleugnung ihres Wahrheitssinns und ihrer Ueberzeugung als Helfer dienen wollten*", wie bspw die Professoren *Wilhelm Eduard Albrecht* (Jurist), *Friedrich C. Dahlmann* (Historiker), *Heinrich Ewald* (Theologe und Orientalist), *Georg G. Gervinus* (Historiker), *Wilhelm E. Weber* (Physiker) sowie *Jacob* und *Wilhelm Grimm* (Ger-

---

* Az. Prof. Dr. *Thomas Kröll* ist assoziierter Professor am Institut für Österreichisches und Europäisches Öffentliches Recht der Wirtschaftsuniversität Wien.

1 Zur Märzrevolution siehe bspw *Huber*, Deutsche Verfassungsgeschichte seit 1789 II[2] (1975) 502-586.

2 Zu den Karlsbader Beschlüssen im Allgemeinen und zum Bundes-Universitätsgesetz im Besonderen siehe bspw *Huber*, Deutsche Verfassungsgeschichte seit 1789 I[2] (1960) 732-739 und 739-742; zur Entstehung *Welcker*, Wichtige Urkunden für den Rechtszustand der deutschen Nation mit eigenhändigen Anmerkungen von Johann Ludwig Klüber[2] (1845).

3 Provisorischer Bundesbeschluß über die in Ansehung der Universitäten zu ergreifenden Maßregeln vom 20. 9. 1819, aufgehoben durch den Bundesbeschluß über die Aufhebung der Bundes-Ausnahmegesetze vom 2. 4. 1848; beide Bundesbeschlüsse abgedruckt bei *Huber*, Dokumente zur deutschen Verfassungsgeschichte I[3] (1978) 101 und 330.

4 *Lehmann*, Die Grundrechte des deutschen Volkes (1850) 56.

Fundstelle: *Kröll*, Der digitalisierte Forscher, ALJ 2/2017, 71–84 (http://alj.uni-graz.at/index.php/alj/article/view/83).

manisten), besser bekannt als die „Göttinger Sieben“,[5] *Robert von Mohl*[6] (Jurist) oder *Karl Theodor Welcker*[7] (Jurist).

Nachdem Unterrichtsminister *Franz von Sommaruga*[8] am 30. 3. 1848 in der Aula der Wiener Universität die Lehr- und Lernfreiheit proklamiert[9] und erste Maßnahmen zu ihrer Verwirklichung gesetzt hatte,[10] sollten im Frühjahr 1849 die von der Deutschen Verfassungsgebenden Nationalversammlung in Frankfurt am Main am 20. 12. 1848 beschlossenen Grundrechte des Deutschen Volkes,[11] *„die ersten parlamentarisch diskutierten und beschlossenen Grundrechte überhaupt*“, so *Wilhelm Brauneder*,[12] und das mit der Märzverfassung[13] am 4. 3. 1849 oktroyierte Grundrechtspatent[14] die Wissenschaftsfreiheit dem akademischen Forscher in Österreich erstmals auch gesetzlich bzw verfassungsgesetzlich garantieren. Beseitigte kurze Zeit später die konservative Reaktion auch die konstitutionelle Errungenschaft dieses Grundrechtes,[15] die zur Durchführung der Wissenschaftsfreiheit getroffenen Maßnahmen sollten Bestand haben,[16] die Universitäten *„zu oberst […] der Pflege echter Wissenschaftlichkeit“*[17] dienen. Seit der Rückkehr zum Konstitutionalismus am 22. 12. 1867[18] wird dem akademischen Forscher – aber nicht nur diesem – in Art 17 Abs 1 StGG[19] die Wissenschaftsfreiheit garantiert, zunächst als staatsgrundgesetzlich gewährleistetes politi-

5 *Sellert*, Göttinger Sieben, in *Cordes/Lück/Werkmüller* (Hrsg), Handwörterbuch zur deutschen Rechtsgeschichte II (2012) 495; und *Huber*, Deutsche Verfassungsgeschichte II[2] 96–106.

6 *Stolleis*, Mohl, Robert von (1799-1875), in *Erler/Kaufmann* (Hrsg), Handwörterbuch zur deutschen Rechtsgeschichte III (1984) 617.

7 *Welker*, Welcker, Karl Theodor (1790–1869), in *Erler†/Kaufmann/Werkmüller* (Hrsg), Handwörterbuch zur deutschen Rechtsgeschichte V (1998) 1251.

8 *Hye*, Sommaruga, Franz Ser Vincenz Emanuel Frh von, in Österreichische Akademie der Wissenschaften (Hrsg), Österreichisches Biographisches Lexikon 1815-1950 XII (58. Lfg 2005) 411.

9 Rede abgedruckt bei *Heintl*, Mittheilungen aus den Universitäts-Acten (1848) Nr 17.

10 Siehe dazu *Kröll* in *Kneihs/Lienbacher* (Hrsg), Rill-Schäffer-Kommentar zum Bundesverfassungsrecht (13. Lfg 2014) Art 17 Abs 1, 5 StGG Rz 4.

11 Art VI § 22 Reichsgesetz, betreffend die Grundrechte des deutschen Volkes vom 27. 12. 1848 RGBl 1848, 49; am 17. 1. 1849 in Kraft getreten gem Art I Z 10 Einführungsgesetz RGBl 1848, 57.

12 *Brauneder*, Die Gesetzgebungsgeschichte der österreichischen Grundrechte, in *Machacek/Pahr/Stadler* (Hrsg), Grund- und Menschenrechte in Österreich I (1991) 189 (235).

13 Kaiserliches Patent vom 4. 3. 1849, die Reichsverfassung für das Kaiserthum Österreich enthaltend RGBl 1948/150.

14 § 3 Satz 1 Kaiserliches Patent vom 4. 3. 1849, über die, durch die constitutionelle Staatsform gewährleisteten politischen Rechte RGBl 1849/151. Zur Entstehung, zum Wesen und Wirken und zur Durchsetzbarkeit der Grundrechte des Patentes siehe *Brauneder* in *Machacek/Pahr/Stadler* 243–248 und 258–262.

15 Das Reichsgesetz, betreffend die Grundrechte des deutschen Volkes vom 27. 12. 1848 wurde durch den Bundesbeschluss über die Aufhebung der Grundrechte des deutschen Volkes vom 23. 8. 1851 vom Bundestag außer Kraft gesetzt; abgedruckt bei *Huber*, Dokumente zur deutschen Verfassungsgeschichte I[3] (1986) 2. Das Grundrechtspatent vom 4. 3. 1849 wurde am 1. 1. 1852 durch die sog Sylvesterpatente vom 31. 12. 1851 aufgehoben; Kaiserliche Patente vom 31. 12. 1851 RGBl 1852/2 und 1852/3.

16 Provisorisches Gesetz über die Organisation der akademischen Behörden RGBl 1849/401; Allgemeine Anordnungen über das Studienwesen an der juridisch-staatswissenschaftlichen, medizinisch-chirurgischen und philosophischen Facultät der k. k. Universitäten für das Studienjahr 1849–50 RGBl 1849/416 Blg 1; und Provisorische Disciplinar-Ordnung für die Universitäten RGBl 1849/416 Blg 2.

17 § 1 Provisorische Disciplinar-Ordnung für die Universitäten.

18 Gesetz vom 21. 12. 1867, womit der Zeitpunkt bestimmt wird, mit welchem das Gesetz, wodurch das Grundgesetz über die Reichsvertretung vom 26. 2. 1861 abgeändert wird, das Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger für die im Reichsrathe vertretenen Königreiche und Länder, das Staatsgrundgesetz über die Einsetzung eines Reichsgerichtes, das Staatsgrundgesetz über die richterliche Gewalt, das Staatsgrundgesetz über die Ausübung der Regierungs- und der Vollzugsgewalt, endlich das Gesetz, betreffend die allen Ländern der österreichischen Monarchie gemeinsamen Angelegenheiten und die Art ihrer Behandlung, in Wirksamkeit zu treten haben RGBl 1867/147.

19 Staatsgrundgesetz vom 21. 12. 1867 über die allgemeinen Rechte der Staatsbürger für die im Reichsrathe vertretenen Königreiche und Länder RGBl 1867/142.

sches Recht im Sinne der Rsp des k. k. Reichsgerichtes,[20] mit dem Inkrafttreten der Bundesverfassung am 10. 11. 1920 als verfassungsgesetzlich gewährleistetes Recht iSd Art 144 B-VG.[21,22]

Seit nahezu 150 Jahren steht die Wissenschaftsfreiheit nunmehr mit unverändertem normativem Gehalt in Geltung. Ihr Schutzbereich entspricht auch heute noch dem Schutzbereich, der vom Verfassungsausschuss der Deutschen Verfassungsgebenden Nationalversammlung in Frankfurt am Main 1848 erstmals formuliert und vom Staatsgrundgesetzgeber des Jahres 1867 konstituiert worden ist.

Der Schutzzweck besteht – die Entstehungsgeschichte der Wissenschaftsfreiheit belegt dies deutlich – seit jeher in der Anerkennung der Eigengesetzlichkeit[23] der Wissenschaft, präziser: einer jeder *Fach*wissenschaft, die – wegen dieser Eigengesetzlichkeit – der rechtlichen Regelung und Nachprüfung entzogen ist.[24] *Erich Kaufmann* hat im gegebenen Zusammenhang von den „*ewigen Grenzen des Recht[e]s*" gesprochen.[25] Die Wissenschaftsfreiheit ist eine Reaktion auf die staatliche Bevormundung; sie bedeutet zugleich aber auch Emanzipation von kirchlicher Beeinflussung. Weder der Staat, noch eine gesetzlich anerkannte Kirche oder Religionsgesellschaft oder eine Religionsgemeinschaft oder andere gesellschaftliche Kräfte sollen beurteilen, ob eine Tätigkeit – ihr ernsthafter Versuch – und ihre Ergebnisse materiell wissenschaftlichen Anforderungen entsprechen, ob die Wahrheitssuche also erfolgreich war. Dies haben vielmehr die – insoweit sachverständigen – Vertreter der jeweiligen Fachwissenschaft zu entscheiden.[26] *Ignaz Lehmann*, einer der ersten Kommentatoren der Grundrechte des Deutschen Volkes, hat dies bereits 1849 in aller Deutlichkeit formuliert: „*Dem Unrechten und Wahren in der wissenschaftlichen Forschung wird es überall, da wo Freiheit herrscht, an kampfgewachsenen, gleichen Gegnern nicht fehlen, die es bekämpfen; und die Wahrheit bricht sich mit ihrer eigenen Kraft durch allen Irrthum hindurch von selbst die Bahn. Darum soll der Staat nicht das, was ihm an den Ergebnissen der Wissenschaft nicht […] behagt, mit roher äußerer Gewalt niederhalten dürfen.*"[27] Der Wissenschaftsbegriff des StGG ist daher nicht nur ein formeller, würde doch die Aufnahme materieller Kriterien in diesen eine Einmischung der Rechtswissenschaft in den Bereich anderer Fachwissenschaften bewirken. Er ist auch ein materiell offener und wertneutraler Wissenschaftsbegriff. Der Schutz des Art 17 Abs 1 StGG soll nicht nur der Wissenschaft bzw der wissenschaftlichen Tätigkeit und den dabei erlangten Ergebnissen zukommen, die für gesellschaftlich wertvoll oder politisch wünschenswert erachtet werden, son-

20 Zur Rsp des k. k. Reichsgerichtes siehe *Hye* 2135/1914.

21 Art 144 Abs 1 iVm Art 149 Abs 1 B-VG und Art 17 Abs 1 StGG.

22 VfSlg 493/1925 und 3191/1957.

23 „*Der Wesensgrund der Freiheit der Wissenschaft und ihrer Lehre liegt darin, daß die Wissenschaft […] besonderen, nicht aus der staatlichen Gemeinschaft und deren Befugnissen abzuleitenden Gesetzmäßigkeiten unterliegt und daher auch in ihren Institutionen das jenen Gesetzlichkeiten entsprechende Maß von Selbstbestimmung haben muß. Diese Gesetzlichkeit besteht in dem Anspruch der auf rationalem Weg erkennbaren und erkannten Ergebnisse der Wissenschaft auf Allgemeingültigkeit*" so *Meister*, Lehr- und Lernfreiheit in der Thunschen Universitätsreform und in der Gegenwart in Österreich (1957) 214.

24 So auch *Smend*, Das Recht der freien Meinungsäußerung, in VVDStRL 4 (1928) 44 (61); siehe bereits die Beratungen im Verfassungsausschuss der Deutschen Verfassungsgebenden Nationalversammlung und den Bericht des Verfassungsausschusses in *Droysen* (Hrsg), Die Verhandlungen des Verfassungs-Ausschusses der deutschen Nationalversammlung Teil 1 (1849) 19; und *Wigard* (Hrsg), Stenographischer Bericht über die Verhandlungen der Deutschen Constituierenden Nationalversammlung zu Frankfurt am Main III (1848) 2167 f.

25 *Kaufmann*, Untersuchungsausschuß und Staatsgerichtshof (1920) 80.

26 So bereits *Kröll* in *Kneihs/Lienbacher* Art 17 Abs 1, 5 StGG Rz 22 mit Verweis auf *Smend*, VVDStRL 4 (1928) 61; und *Meister*, Lehr- und Lernfreiheit 214 f.

27 *Lehmann*, Grundrechte 57.

dern auch jenen, die für bestimmte gesellschaftliche Gruppen schockierend, aus heutiger Sicht nutzlos oder ethisch bedenklich sind.[28]

In sachlicher Hinsicht erfasst der Schutzbereich die selbständige wissenschaftliche Forschung, dh die freie Wahl des Gegenstandes, der zu behandelnden Fragen und der Methoden der Forschung, die Durchführung der Forschungsarbeiten, die Aufzeichnung und Bewertung der Forschungsergebnisse und ihre Darstellung in selbstgewählter Form. Neben dem damit umschriebenen Werkbereich umfasst der Wirkbereich der Wissenschaftsfreiheit die schriftliche und mündliche Vertretung sowie die Verbreitung der Forschungsergebnisse in selbstgewählter Form, wie bspw durch Monographie, Zeitschriftenbeitrag, Vortrag oder Blog.[29]

In persönlicher Hinsicht erfasst der Schutzbereich jede natürliche Person, zuvorderst den akademischen, an einer öffentlichen Universität tätigen Forscher. Wer an einer öffentlichen Universität nun zur selbständigen Forschung berechtigt und regelmäßig auch verpflichtet ist, ergibt sich aus organisationsrechtlichen, dienst- bzw arbeitsrechtlichen und studienrechtlichen Bestimmungen. Der so einfachgesetzlich Berechtigte und Verpflichtete kann sich auch der öffentlichen Universität gegenüber auf die Wissenschaftsfreiheit berufen, wenn er dort selbständig forscht.[30] In Betracht kommen nicht nur Professoren,[31] sondern auch, was bisweilen verkannt wird, wissenschaftliche Mitarbeiter, sind diese doch nicht nur zur Mitarbeit an den Forschungsaufgaben der jeweiligen Organisationseinheit, der sie zugeordnet sind, verpflichtet, sondern nach Kollektiv- und Individualarbeitsvertrag auch zur selbständigen wissenschaftlichen Forschung berechtigt und verpflichtet,[32] und Studienende, insb Dissertanten.[33,34]

Art 17 Abs 1 StGG erschöpft sich aber nicht in seinem abwehrrechtlichen Gehalt, sondern begründet darüber hinaus, ergänzt durch Art 81c B-VG,[35] auch Gewährleistungspflichten in Form positiver Schutzpflichten.[36] Schon während der Geltung der Dezemberverfassung sollten die Grundrechte des StGG in erster Linie und unbeschadet ihrer Qualifikation als politische Rechte im Sinne der Rsp des k. k. Reichsgerichtes jene „*Principien [darstellen], von welchen die Gesetzgebung und Verwaltung im Staate gegenüber der Freiheit des einzelnen Staatsbürgers geleitet sein soll*".[37,38] Nunmehr verhalten die positiven Schutzpflichten den Gesetzgeber und die öffentlichen

28 So bereits *Kröll* in *Kneihs/Lienbacher* Art 17 Abs 1, 5 StGG Rz 23 mwN.

29 Zum sachlichen Schutzbereich des Art 17 Abs 1 StGG siehe *Kröll* in *Kneihs/Lienbacher* Art 17 Abs 1, 5 StGG Rz 33–37 mwN.

30 Zum persönlichen Schutzbereich des Art 17 Abs 1 StGG siehe *Kröll* in *Kneihs/Lienbacher* Art 17 Abs 1, 5 StGG Rz 59 f und 65 mwN.

31 § 94 Abs 2 Z 1 iVm § 97 Abs 1 Bundesgesetz über die Organisation der Universitäten und ihre Studien (Universitätsgesetz 2002 – UG) BGBl I 2002/120 idF BGBl I 2017/11; § 25 Abs 1 Z 1 Kollektivvertrag für die ArbeitnehmerInnen der Universitäten 2015 (Fassung mit 6. Nachtrag).

32 § 94 Abs 2 Z 2 iVm § 122 Abs 2 Z 4 und Abs 3–6 (Universitätsdozenten) bzw § 100 Abs 1 UG (wissenschaftliche Mitarbeiter); § 27 Abs 6 und Abs 7 Z 1 (assoziierte Professoren) bzw § 26 Abs 5 Z 1 und 5 Kollektivvertrag für die ArbeitnehmerInnen der Universitäten 2015 (Universitätsassistenten).

33 § 94 Abs 1 Z 1 iVm § 51 Abs 3 UG.

34 Siehe dazu eingehend *Kröll* in *Kneihs/Lienbacher* Art 17 Abs 1, 5 StGG Rz 66–72.

35 *Berka* in *Kneihs/Lienbacher* (Hrsg), Rill-Schäffer-Kommentar zum Bundesverfassungsrecht (12. Lfg 2013) Art 81c B-VG Rz 64, 67 und 69 f; und *Kucsko-Stadlmayer* in *Korinek/Holoubek ua* (Hrsg), Bundesverfassungsrecht (10. Lfg 2011) Art 81c B-VG Rz 35 und 41.

36 Siehe *Kröll* in *Kneihs/Lienbacher* Art 17 Abs 1, 5 StGG Rz 90 mwN.

37 Bericht des Verfassungsausschusses des Abgeordnetenhauses zum StGG; abgedruckt in Die neue Gesetzgebung Österreichs. Erläutert aus den Reichsraths-Verhandlungen I (1868) 310.

38 Siehe bspw auch *Göllerich*, Die Grundrechte der österreichischen Staatsbürger nach dem Staats-Grundgesetze vom 21. 12. 1867 (1868) 27; und Der Einfluß der Staatsgrundgesetze vom 21. 12. 1867 (Nr 142, 143, 144 RGB) auf

Universitäten zu einer „wissenschaftsadäquaten“[39] Ausgestaltung der Universitätsorganisation, des Dienst- und Arbeitsrechtes der Angehörigen des wissenschaftlichen Universitätspersonals und des Studienrechtes. „Wissenschaftsadäquat“ ist eine Ausgestaltung aber nur, wenn sie im Sinne des Schutzzweckes des Art 17 Abs 1 StGG die Eigengesetzlichkeit der Wissenschaft – präziser: einer jeden Fachwissenschaft – respektiert und garantiert und jede Fremdbestimmung ausschließt,[40] woher diese auch kommen mag – vom Staat, von einer gesetzlich anerkannten Kirche oder Religionsgesellschaft, von einer Religionsgemeinschaft, von der Universität selbst, ihren Organen, Verwaltungseinrichtungen oder inneruniversitären Gruppen, von Parteien und Interessenverbänden oder von anderen gesellschaftlichen Kräften.

Die Wissenschaftsfreiheit ist kein unbeschränkt gewährleistetes und unbeschränkbares Grundrecht. Ihre Vorbehaltslosigkeit bedeutet nicht auch ihre Schrankenlosigkeit. Art 17 Abs 1 StGG enthält vielmehr immanente Grundrechtsschranken.[41] Die Wissenschaftsfreiheit untersagt zum einen intentional und direkt auf eine Beschränkung der wissenschaftlichen Forschung gerichtete Regelungen.[42] Zum anderen steht die Wissenschaftsfreiheit allgemeinen – auch den wissenschaftlichen Forscher bindenden – Gesetzen entgegen, wenn diese der Verhältnismäßigkeitsprüfung nicht standhalten.[43] Was endlich universitätsorganisationsrechtliche, spezifisch an die Angehörigen des wissenschaftlichen Universitätspersonals gerichtete dienst- bzw arbeitsrechtliche und studienrechtliche Regelungen anlangt, sind diese regelmäßig nicht als allgemeine Gesetze zu qualifizieren. Sie beziehen sich nämlich nur auf die Angehörigen des wissenschaftlichen Universitätspersonals bzw auf deren zentrale Tätigkeiten – die wissenschaftliche Forschung und Lehre. Mit diesen Regelungen verfolgen Gesetzgeber und Universitätsorgane im besonderen Interesse gelegene Ziele wie bspw die „wissenschaftsadäquate“ Organisation der staatlich finanzierten öffentlichen Universitäten, die Sicherstellung der Einstellung von hervorragend fachlich-wissenschaftlich qualifiziertem Personal oder die Entwicklung der Wissenschaften bzw die Entwicklung und Entschließung der Künste, die wissenschaftliche Berufsausbildung oder ein geordneter Lehr- und Studienbetrieb. Diese die äußere Ordnung der wissenschaftlichen Forschung und Lehre an öffentlichen Universitäten[44] bildenden nicht intentional und direkt auf eine Beschränkung der wissenschaftlichen Forschung gerichteten, nicht allgemeinen, sondern besonderen Gesetze sind nur dann zulässig, wenn sie zum Schutz eines besonderen öffentlichen Interesses erforderlich und verhältnismäßig sind. Sie sind im Einzelfall stets darauf hin zu überprüfen, ob sie nicht doch intentional und direkt auf eine Beschränkung der Wissenschaftsfreiheit gerichtet sind oder es zumindest ermöglichen, Forschung und Lehre im Hinblick auf ihre Zwecke, Inhalte oder Methoden intentional und direkt zu beeinflussen, zu beschränken oder gar zu unterdrücken.

---

die österreichische Gesetzgebung (Separatabdruck aus der „Allgemeinen Österreichischen Gerichtszeitung“) (1868) 6 und 25.

39 *Pöschl*, Von der Forschungsethik zum Forschungsrecht: Wie viel Regulierung verträgt die Forschungsfreiheit? in *Körtner/Kopetzki/Druml* (Hrsg), Ethik und Recht in der Humanforschung (2010) 90 (116).

40 *Kröll* in *Kneihs/Lienbacher* Art 17 Abs 1, 5 StGG Rz 92 mit Verweis auf *Berka*, Die Gewährleistung der Wissenschaftsfreiheit in privaten Bildungseinrichtungen, in FS Adamovich (2002) 45 (51); und *Berka*, Autonomie im Bildungswesen, in *Brünner/Mantl/Welan* (Hrsg), Studien zu Politik und Verwaltung (2002) 38 und 40.

41 Siehe dazu bspw *Kröll* in *Kneihs/Lienbacher* Art 17 Abs 1, 5 StGG Rz 117 und 119 mwN.

42 *Kröll* in *Kneihs/Lienbacher* Art 17 Abs 1, 5 StGG Rz 123–127.

43 *Kröll* in *Kneihs/Lienbacher* Art 17 Abs 1, 5 StGG Rz 128 f und zum Begriff „allgemeines Gesetz“ Rz 130 f.

44 *Kröll* in *Kneihs/Lienbacher* Art 17 Abs 1, 5 StGG Rz 132-139.

II. Von Georg Beseler ins 21. Jahrhundert …

Als *Georg Beseler*,[45] selbst Professor der Rechte in Greifswald, am 6. 6. 1848 im Verfassungsausschuss der Deutschen Verfassungsgebenden Nationalversammlung in Frankfurt am Main den Satz „*Die Wissenschaft und ihre Lehre ist frei*" formulierte,[46] der in Folge erstmals Gesetz werden sollte, konnte er wohl kaum erahnen, welche gesellschaftlichen und technologischen Entwicklungen noch im 19., im 20. und im frühen 21. Jahrhundert stattfinden sollten und wie sich – in Anbetracht der sich stets beschleunigenden Technisierung und Digitalisierung des täglichen Lebens eines jeden Einzelnen – im Frühjahr 2017 die Rahmenbedingungen für den akademischen Forscher gestalten würden. Die sich nunmehr bietenden Möglichkeiten digitaler Präsenz und digitaler Informationsbeschaffung hätten *Beseler* sicherlich begeistert. Er fand zwar in Greifswald, einer kleinen Universitätsstadt am Rande des Geschehens ohne große Ablenkungsmöglichkeiten, ein ideales Arbeitsklima vor.[47] Der Zustand der Universität im Allgemeinen und seine Arbeitsbedingungen im Besonderen mussten aber alles andere als ideal gewesen sein, ließ er doch kurz nach seiner Ankunft in Greifswald seinen Jugendfreund *Gervinus* wissen, *„[die] Universität [sei] ein rotten borough der allerärgsten Sorte*".[48] In kluger Voraussicht hatte er sich zusichern lassen, die Bibliothek der Berliner Universität nutzen zu dürfen;[49] in den Ferien nutzte er zudem gelegentlich jene der Universität Göttingen[50] – damals nicht gerade ein Katzensprung. Einem gesetzlichen Gebot zur Evaluierung der Aufgaben und Leistungen der öffentlichen Universität, insb der Leistungen der Angehörigen des wissenschaftlichen Universitätspersonals in Forschung und Lehre, unter Nutzung der sich nunmehr bietenden technischen Möglichkeiten, wäre *Beseler* – gerade nach der Befreiung von staatlicher Bevormundung – wohl skeptisch gegenübergestanden.

III. … zum digital informierten Forscher

Die stete Zunahme digitalisierter Informationen und ihre leichtere Auffindbarkeit und Zugänglichkeit sind ein unbestreitbarer Vorteil der Digitalisierung. Der akademische Forscher ist heute zunehmend digital informiert.

Im Falle des Rechtswissenschaftlers betrifft dies zunächst seinen Erkenntnisgegenstand – das positive österreichische Recht und das Recht der Europäischen Union.

Seit Juni 1997 informiert das Rechtsinformationssystem des Bundes (RIS) in seiner Gestalt als vom Bundeskanzleramt betriebene, für jedermann zugängliche, kostenfrei abrufbare Internetapplikation über das österreichische Recht.[51] Seine Anfänge reichen bis in das Jahr 1981 zurück. Angesichts der stetig wachsenden Zahl an Rechtsvorschriften sollte ein elektronisches System eingerichtet werden, um die Suche nach dem Recht, insb nach seiner geltenden Fassung, zu vereinfachen und zu beschleunigen. Damit sollte die Zeit, in der allein das Auffinden der geltenden

45 *Kern*, Beseler, Georg (1809–1888), in *Cordes/Lück/Werkmüller* (Hrsg), Handwörterbuch zur deutschen Rechtsgeschichte I (2008) 546. Siehe eingehend *Kern*, Georg Beseler – Leben und Werk (1982).

46 Siehe die Beratungen im Verfassungsausschuss der Deutschen Verfassungsgebenden Nationalversammlung: „[*Beseler] schlägt vor: ‚Die Wissenschaft und ihre Lehre ist frei.'*" *Beseler* in *Droysen* 19.

47 *Kern*, Germanisten versus Romanisten: Georg Beseler (1809–1888), in *Lege* (Hrsg), Greifswald – Spiegel der deutschen Rechtswissenschaft 1815 bis 1945 (2009) 113 (120).

48 *Kern*, Leben 68 FN 12.

49 *Kern*, Leben 68.

50 *Kern*, Leben 500.

51 Siehe http://www.ris.bka.gv.at/default.aspx (abgefragt am 4. 5. 2017).

Rechtslage in einem etwas entlegeneren Fachgebiet stundenlange Recherche in einer Bibliothek, gar im Archiv, erforderte, der Vergangenheit angehören.[52]

Mit dem RIS und seinen vielfältigen Applikationen, der seit 2004 bzw 2014[53] und 2015[54] ebendort papierlos erfolgenden Kundmachung der Rechtsvorschriften des Bundes und der Länder in den nunmehr elektronischen Gesetzblättern[55] und der RIS-App,[56] die es ermöglicht, auch unterwegs auf Smartphone oder Tablet auf österreichische Rechtsvorschriften zuzugreifen, ist der vorläufige Endpunkt in der Entwicklung der Rechtsinformation erreicht. Diese Entwicklung hat Mitte des 17. Jahrhunderts mit der Herausgabe der ersten privaten Gesetzessammlung, des „Codex Ferdinandeus", durch den Kanzler der Niederösterreichischen Regierung *Johann Baptist Suttinger*[57] begonnen.[58] Sie führte über weitere private Sammlungen mit zum Teil offiziösem Anstrich, wie jenen des Hofsekretärs *Joseph Kropatschek*,[59] in einem ersten Schritt zu den seit dem Ende des 18. Jahrhunderts unter Kaiser *Joseph II.* von den staatlichen Behörden selbst herausgegebenen offiziellen Gesetzessammlungen, der Justizgesetzessammlung ab 1876 und der Politischen Gesetzessammlung 1890,[60] und einem zweiten Schritt zur Kundmachung der Rechtsvorschriften in den 1849 erstmals eingeführten Reichs- und den Landesgesetzblättern.[61] Sie brachte schließlich, im Jahr 2002, erstmals eine papierlose Kundmachung von Rechtsvorschriften – der Durchführungsvorschriften der Sozialversicherungsträger und des Hauptverbandes zu den Sozialversicherungsgesetzen – im Internet[62] hervor. Der tägliche Gebrauch des RIS und seiner vielfältigen Applikationen ist für jeden österreichischen Rechtswissenschaftler eine Selbstverständlichkeit. Wer sich einmal auf die Suche nach ausländischen, bspw italienischen Rechtsvorschriften in ihrer geltenden Fassung machen musste, lernt erst seine Qualität schätzen.

Auch das historische, nicht mehr in Geltung stehende österreichische Recht ist dem interessierten Rechtswissenschaftler in digitaler Form zugänglich. ALEX, der digitale Lesesaal der Österreichischen Nationalbibliothek, dokumentiert nicht nur den staatlichen Normausstoß vergangener staatlicher Epochen, sondern bildet auch eine hervorragende Quelle für Forschung zu Geschichte, Politik, Kultur und Gesellschaft.[63]

In einer dem RIS vergleichbaren Weise ermöglicht das vom interinstitutionellen Amt für Veröffentlichungen der Europäischen Union betriebene EUR-Lex jedermann einen kostenfreien Zugriff

52 *Forgó/Holzweber*, Vom EDV-Versuchsprojekt „Verfassungsrecht" zum Rechtsinformationssystem des Bundes, in FS Lachmayer (2014) 257; und *Weichsel*, Rechtsinformationssystem (RIS) – Ein Rück- und Ausblick, in FS Lachmayer (2014) 185 (185–188).

53 Kärnten, Steiermark, Tirol und Wien.

54 Burgenland, Niederösterreich, Oberösterreich, Salzburg und Vorarlberg.

55 Kundmachungsreformgesetz 2004 BGBl I 2003/100; ErläutRV 93 BlgNR 22. GP 3 ff; Verwaltungsgerichtsbarkeits-Novelle 2012 BGBl I 2012/51; ErläutRV 1618 BlgNR 24. GP 11; und *Rosner*, Authentische Kundmachung der Landesgesetzblätter im Rechtsinformationssystem des Bundes, in FS Lachmayer (2014) 661.

56 Siehe http://www.ris.bka.gv.at/UI/RISApp.aspx (abgefragt am 4. 5. 2017).

57 *Neschwara*, Johann Baptist Suttinger (1608–1662), in FS Brauneder (2008) 363.

58 *Pauser*, Landesfürstliche Gesetzgebung (Policey-, Malefiz- und Landesordnungen), in *Pauser/Scheutz/Winkelbauer* (Hrsg), Quellenkunde der Habsburgermonarchie (16.-18. Jahrhundert) (2004) 216 (234 f).

59 *Pauser* in *Pauser/Scheutz/Winkelbauer* 235–238.

60 *Pauser* in *Pauser/Scheutz/Winkelbauer* 238 f.

61 Kaiserliches Patent vom 4. 3. 1849, wodurch die Einführung eines allgemeinen Reichs-Gesetz- und Regierungsblattes sowie der Landes-Gesetz- und Regierungsblätter angeordnet wird RGBl 1849/153.

62 58. Novelle zum ASVG BGBl I 2001/99; und 59. Novelle zum ASVG BGBl I 2002/1. Siehe *Souhrada*, www.avsv.at: Amtliche Verlautbarungen der Sozialversicherung im Internet, SoSi 2002, 6.

63 Siehe http://alex.onb.ac.at (abgefragt am 4. 5. 2017).

auf das Unionsrecht in den 24 Amtssprachen.[64] Seit 1. 7. 2013 erfolgt im Rahmen des EUR-Lex zudem die papierlose Kundmachung des Unionsrechtes im elektronischen Amtsblatt.[65]

Eine Vielzahl in ihrem Umfang variierender elektronischer Kataloge und elektronischer Suchmaschinen mit unterschiedlicher Reichweite und raffinierten Suchoptionen erleichtern dem Rechtswissenschaftler die Auffindbarkeit von ihm gezielt oder großflächig gesuchter Literatur. Mehr oder weniger spezialisierte Datenbanken eröffnen ihm den – an sich meist kostenpflichtigen, für ihn aber regelmäßig kostenfreien – Zugriff auf diese Literatur in digitaler Form direkt an seinem Arbeitsplatz, wo auch immer sich dieser befindet – im Büro, zu Hause oder unter der Sonne Kärntens.

Neben dem positiven Recht als Erkenntnisgegenstand und der rechtswissenschaftlichen Literatur kommen freilich noch andere Informationen, auch solche in digitaler Form, als Grundlage rechtswissenschaftlicher Forschung in Betracht. Sind diese im Besitz von staatlichen Organen, Einrichtungen oder Unternehmungen – wie bspw von diesen erstellte oder in Auftrag gegebene Gutachten, Studien oder Statistiken – oder von Privaten und daher für den Rechtswissenschaftler nicht zugänglich, verleiht Art 17 Abs 1 StGG kein verfassungsgesetzlich gewährleistetes Recht auf Zugang zu diesen Informationen. Die Wissenschaftsfreiheit impliziert keine Informationszugangsfreiheit – weder gegenüber dem Staat, seinen Organen, Einrichtungen und Unternehmungen, noch gegenüber Privaten.[66] Sie ist auch zu keinem Zeitpunkt in einem solchen Sinne verstanden worden.[67]

Solange nicht ein verfassungsgesetzlich gewährleistetes Recht auf Zugang zu Informationen – möglicherweise in Kombination mit einer staatlichen Informationsverpflichtung – Verfassungswirklichkeit geworden ist,[68] bleiben im Hinblick auf den Zugang zu Informationen, die sich im Besitz von staatlichen Organen, Einrichtungen oder Unternehmungen befinden, auch weiterhin Art 20 Abs 3 und 4 B-VG betreffend Auskunftspflicht und Amtsverschwiegenheit der Verwaltungsorgane[69] und die dazu ergangenen Ausführungsgesetze maßgeblich.

Neben den allgemeinen Auskunftspflichtgesetzen des Bundes[70] und der Länder,[71] die ein allgemeines einfachgesetzliches Informationsrecht begründen, sind dies insb das Umweltinformations-

64 Art 3 Abs 1 lit a und f Beschluss 2009/496/EG, Euratom des Europäischen Parlaments, des Rates, der Kommission, des Gerichtshofs, des Rechnungshofs, des Europäischen Wirtschafts- und Sozialausschusses und des Ausschusses der Regionen vom 26. 6. 2009 über den Aufbau und die Arbeitsweise des Amtes für Veröffentlichungen der Europäischen Union ABl L 2009/168, 41.

65 Art 1 VO (EU) 216/2013 des Rates vom 7. 3. 2013 über die elektronische Veröffentlichung des Amtsblatts der Europäischen Union ABl L 2013/69, 1.

66 Zum sachlichen Schutzbereich der Wissenschaftsfreiheit siehe FN 29.

67 Siehe FN 24.

68 Siehe RV 395 und ErläutRV 395 BlgNR 25. GP zum Entwurf eines Bundesverfassungsgesetzes, mit dem das Bundes-Verfassungsgesetz geändert wird, mit dem die Amtsverschwiegenheit abgeschafft und eine Informationsverpflichtung und ein verfassungsgesetzlich gewährleistetes Recht auf Zugang zu Informationen geschaffen werden soll.

69 Siehe dazu *Mayer/Kucsko-Stadlmayer/Stöger*, Bundesverfassungsrecht[11] (2015) Rz 582–586/6; und *Mayer/Muzak*, Das österreichische Bundes-Verfassungsrecht Kurzkommentar[5] (2015) Art 20 B–VG B und C.

70 Bundesgesetz vom 15. 5. 1987 über die Auskunftspflicht der Verwaltung des Bundes und eine Änderung des Bundesministeriengesetzes 1986 (Auskunftspflichtgesetz) BGBl 1987/287 idF BGBl I 1998/158.

71 Gesetz vom 14. 12. 2006 über die Auskunftspflicht, die Weiterverwendung von Informationen öffentlicher Stellen sowie die Statistik des Landes Burgenland (Bgld Auskunftspflicht-, Informationsweiterverwendungs- und Statistikgesetz – Bgld AISG) LGBl 2007/14 idF LGBl 2015/31; Gesetz vom 7. 7. 2005 über Auskunftspflicht, Datenschutz und Statistik des Landes (Krnt Informations- und Statistikgesetz – K-ISG) LGBl 2005/70 idF LGBl 2016/22; NÖ Auskunftsgesetz LGBl 0020–4 idF LGBl 2015/58; Landesgesetz über die Auskunftspflicht, den Datenschutz und die Weiterverwendung von Informationen öffentlicher Stellen (Oö Auskunftspflicht-, Datenschutz- und Informationsweiterverwendungsgesetz) LGBl 1988/46 idF LGBl 2015/68; Sbg Gesetz über Auskunftspflicht, Dokumentenweiter-

gesetz[72] und das Informationssicherheitsgesetz,[73] die – freilich lediglich punktuell – besondere einfachgesetzliche Informationsrechte verleihen.

IV. … zum digital evaluierten Forscher

Die gesetzlich gebotene Evaluierung der Leistungen der Angehörigen des wissenschaftlichen Universitätspersonals in Forschung und Lehre erfordert diese betreffende Informationen. Stehen diese Informationen auch in digitaler Form zur Verfügung, ist die Evaluierung des akademischen Forschers mitunter eine digital abgestützte.

§ 14 Universitätsgesetz 2002[74] ordnet die Evaluierung des gesamten Leistungsspektrums der öffentlichen Universitäten im Rahmen eines einzurichtenden Qualitätsmanagementsystems zur Leistungs- und Qualitätssicherung an. Gegenstand der Evaluierung, die nach fachbezogenen internationalen Standards zu erfolgen hat, sollen insb die Leistungen der Angehörigen des wissenschaftlichen Universitätspersonals in Forschung und Lehre sein.

§ 14 Universitätsgesetz 2002 und die zu seiner Durchführung ergehenden Satzungen der öffentlichen Universitäten sind Bausteine der äußeren Ordnung der wissenschaftlichen Forschung und Lehre. Sie beziehen sich auf die Angehörigen des wissenschaftlichen Universitätspersonals und ihre zentralen Tätigkeiten und sind damit als einem besonderen öffentlichen Interesse – einer näher zu definierenden „Qualität" wissenschaftlicher Forschung und Lehre – dienende besondere Gesetze zu qualifizieren. Als solche sind sie „wissenschaftsadäquat", präziser: „fachwissenschaftsadäquat", auszugestalten. Dies gilt insb für Vorschriften, die Ziele, Kriterien, Verfahren und Kontrolle der Evaluierung der Leistungen des wissenschaftlichen Universitätspersonals in Forschung und Lehre betreffen.

Die Rechtswissenschaft zeichnet sich durch ihren Erkenntnisgegenstand – je nach Rechtsmaterie innerstaatliches, europäisches und/oder internationales „Recht" – und die diesen betreffende Rechtsdogmatik aus. Dies hat gewisse Eigengesetzlichkeiten rechtswissenschaftlicher Forschung – nicht nur in Österreich, sondern europaweit – im Vergleich zu anderen Fachwissenschaften hervorgebracht. Diese Eigengesetzlichkeiten kommen zum einen in Besonderheiten zum Ausdruck, die die Publikationstätigkeit betreffen. Monographien und Kommentarliteratur, aber auch Beiträgen in Fachzeitschriften und Sammelbänden wird hohe Bedeutung beigemessen. Dagegen existieren nur wenige rein elektronische und unter diesen kaum offene Publikationsmedien. Eine Klassifizierung von Zeitschriften erfolgt nicht. Zum anderen stützt sich die Messung rechtswissenschaftlicher Forschungsleistungen nach wie vor auf eine qualitative Beurteilung, insb durch Herausgeber oder Schriftleiter von Publikationsmedien oder durch Gutachter in Habilitations-

verwendung, Datenschutz, Landesstatistik und Geodateninfrastruktur LGBl 1988/73 idF LGBl 2015/59; Gesetz vom 26. 6. 1990 über die Erteilung von Auskünften (Stmk Auskunftspflichtgesetz) LGBl 1990/73 idF LGBl 2013/87; Gesetz vom 16. 11. 1988 über die Auskunftspflicht der Organe des Landes, der Gemeinden, der Gemeindeverbände und der übrigen durch Landesgesetz geregelten Selbstverwaltungskörper (Tir Auskunftspflichtgesetz) LGBl 1989/4 idF LGBl 2012/150; Vbg Gesetz über die Auskunftserteilung in der Verwaltung des Landes und der Gemeinden LGBl 1989/17 idF LGBl 2013/44; und Gesetz über die Auskunftspflicht (Wr Auskunftspflichtgesetz) LGBl 1999/29 idF LGBl 2013/33.

72 § 1 Z 1 iVm § 4 Bundesgesetz über den Zugang zu Informationen über die Umwelt (Umweltinformationsgesetz – UIG) BGBl 1993/495 idF BGBl I 2015/95.

73 § 3 Abs 1 Z 2 Bundesgesetz über die Umsetzung völkerrechtlicher Verpflichtungen zur sicheren Verwendung von Informationen (Informationssicherheitsgesetz – InfoSiG) BGBl I 2002/23 idF BGBl I 2006/10.

74 Siehe dazu ErläutRV 1134 BlgNR 21. GP 75.

und Berufungsverfahren. Eine quantitative Messung wissenschaftlicher Forschungsleistungen hat demgegenüber in der Rechtswissenschaft nahezu keine Tradition. Es fehlen dafür vielfach die tatsächlichen Voraussetzungen. Einschlägige elektronische Messverfahren existieren für andere Fachwissenschaften, nicht aber für die Rechtswissenschaft; eine Messung rechtswissenschaftlicher Forschungsleistungen anhand solcher Verfahren ist weder möglich noch zielführend. Eine „rechtswissenschaftsadäquate" Ausgestaltung von Vorschriften, die Ziele, Kriterien, Verfahren und Kontrolle der Evaluierung der rechtswissenschaftlichen Forschungsleistungen betreffen, muss diesen Eigengesetzlichkeiten Rechnung tragen.

Als Evaluierungsziele werden in den Satzungen regelmäßig die Feststellung, Sicherung und Entwicklung der – auch hier noch nicht näher definierten – „Qualität" der Leistungen in Forschung und Lehre, die Selbsteinschätzung der Angehörigen des wissenschaftlichen Universitätspersonals sowie die Bereitstellung von Informationen über die Leistungen in Forschung und Lehre zur mittel- und langfristigen Planung und zur Rechenschaftslegung gegenüber der Öffentlichkeit genannt.[75]

Was unter „Qualität" zu verstehen ist, lässt sich in der Regel erst aus den zumeist in universitären Planungsdokumenten, zuvorderst den Entwicklungsplänen und Zielvereinbarungen mit Organisationseinheiten und deren Angehörigen, enthaltenen Evaluierungskriterien erschließen. Als solche kommen, was Publikationen betrifft, qualitative, quantitative, ihre Verbreitung betreffende und ihren wissenschaftlichen oder gesellschaftlichen „Impact" messende Kriterien in Betracht. Sodann kommen Kriterien in Frage, die sich auf den Wissenstransfer beziehen, wie bspw die Organisation und Teilnahme an wissenschaftlichen Konferenzen und deren Häufigkeit, die Einladung zu Vorträgen und deren Häufigkeit, aber auch die Organisation und Teilnahme an Veranstaltungen mit bridging-Funktion zur Praxis oder Etablierung von Kooperationen mit der Praxis. Das gilt auch für Kriterien, welche die Vernetzung betreffen, wie bspw Forschungsaufenthalte im In- und Ausland oder Forschungskooperationen. Zu nennen sind ferner Kriterien, die auf Prämien, Preise und Ehrungen abstellen, oder solche, die sich auf die Einwerbung von Drittmitteln und deren Höhe beziehen. Schließlich können auch Kriterien herangezogen werden, welche die Tätigkeit als Herausgeber, Schriftleiter, Gutachter oder Beirat von wissenschaftlichen Zeitschriften oder als Gutachter in Habilitations- und Berufungsverfahren betreffen. Im Übrigen können Kriterien mit Bezug auf die Ausbildung und Förderung des wissenschaftlichen Nachwuchses, wie bspw Dissertationen und Habilitationen oder Platzierung und Karriereverläufe (ehemaliger) wissenschaftlicher Mitarbeiter, maßgeblich sein. Als Kriterien können aber auch – dies ist nicht ausgeschlossen – die für die Forschung verwendete Arbeitszeit, die Anwesenheit der einzelnen Angehörigen des wissenschaftlichen Personals an ihrem Arbeitsplatz, die Laufzeit des PC, die Zahl einlangender und ausgehender Emails, der Besuch der Bibliothek, die Häufigkeit der Inanspruchnahme von elektronischen Katalogen, Suchmaschinen und Datenbanken oder die Anzahl von Buchausleihen, Fernleihe- und Document Delivery-Bestellungen in Betracht kommen.

Als Quellen für Forschungsleistungen des wissenschaftlichen Universitätspersonals betreffende Informationen, die für die hier beispielhaft angeführten, je nach Kombination einen beliebigen,

75 Siehe bspw § 1 des Teiles „Evaluierung" der Satzung der Universität Graz idF vom 4. 8. 2014; § 52 Abs 6 Satzung der Universität Salzburg idF vom 26. 1. 2016; § 2 des Teiles „Qualitätssicherung" der Satzung der Universität Wien idF vom 29. 3. 2014; und § 2 Anh 3 der „Evaluierungsrichtlinien" der Satzung der Wirtschaftsuniversität Wien idF vom 19. 10. 2016.

mehr oder weniger diffusen Qualitätsbegriff beschreibenden Evaluierungskriterien relevant sind, kommen insb Lebensläufe und Publikationsverzeichnisse der Angehörigen, Tätigkeitsberichte der Organisationseinheiten und deren Angehöriger, auch in digitaler Form, und elektronische Forschungsdokumentationen in Betracht. Informationen bieten zudem, datenschutzrechtliche Fragen seien hier ausgeblendet, elektronische Bibliothekskonten und elektronische Zeiterfassungs- und Zugangssysteme.

Die Wissenschaftsfreiheit steht einer fach- bzw rechtswissenschaftsadäquaten Evaluierung im Sinne einer Abbildung der erbrachten Forschungsleistungen – bspw der Anzahl der Publikationen, besuchter Konferenzen, gehaltener Vorträge, verliehener Preise oder der Höhe eingeworbener Drittmittel – an sich nicht entgegen. Das folgt schon daraus, dass die Wissenschaftsfreiheit ja nicht die Freiheit bedeutet, nicht zu forschen.[76] Der akademische (Rechts-)Wissenschaftler ist und bleibt verpflichtet, sein Fach in der Forschung zu vertreten und zu fördern; er ist ja für dieses verantwortlich. Er darf dahin überprüft werden, ob er seine gesetzliche Verpflichtung erfüllt, ob er überhaupt forscht, publiziert, vorträgt. Dabei ist aber der aus der Wissenschaftsfreiheit resultierende Freiraum zu achten. Erscheint keine Publikation, wird kein Vortrag gehalten, wird der „*im Allgemeinen erzielbare Arbeitserfolg […] nicht erreicht*“[77] – solche Fälle kommen in der Praxis immer wieder vor –, stellt das Dienst- bzw Arbeitsrecht geeignete Mittel zur Verfügung, um solche Pflichtverletzungen abzustellen. Diese sind von den Universitätsorganen und -einrichtungen aber auch zu ergreifen. Dass in solchen Fällen weggeschaut wird, weil der Einsatz dieser Mittel zu langwierig oder mühsam ist, ist schlicht inakzeptabel.

Geht aber mit einer solchen Evaluierung auch eine qualitative Messung der Forschungsleistungen einher, muss auch diese fachwissenschaftsadäquat erfolgen. Eine qualitative Messung von Forschungsleistungen, insb von Publikationen, darf ausschließlich durch Sachverständige, dh durch Vertreter der jeweiligen Fachwissenschaft, erfolgen. Aber selbst dann, wenn eine Forschungsleistung fachintern umstritten ist, bedeutet das nicht, dass keine Forschungsleistung erbracht worden ist. Es kann und darf nur darum gehen, ob überhaupt eine als Forschungsleistung qualifizierbare Leistung erbracht worden ist, nicht aber darum, ob die erlangten Forschungsergebnisse Anerkennung finden oder nicht, ob sie geteilt, bestritten oder verworfen werden. Die Forschungsleistungen eines *Adolf Julius Merkl* zur Frage, ob es im positiven Recht so etwas wie rechtswidriges Recht gibt, zu Fehlerkalkül und Stufenbau der Rechtsordnung, waren zunächst äußerst bestritten; er konnte sie aller Kritik und Anfeindungen zum Trotz dennoch weiterführen. Erst viel später wurden sie als bis heute uneingeholte Pionierarbeit gefeiert.

Solange elektronische Verfahren für eine quantitative Messung von Forschungsleistungen, insb von deren Verbreitung, zwar für andere Fachwissenschaften, nicht aber spezifisch für die Rechtswissenschaft existieren, und solange solche Verfahren nicht eine „wirkungsgerechte“ Abbildung rechtswissenschaftlicher Forschungsleistungen ermöglichen, ist eine quantitative Messung anhand solcher Verfahren nicht nur nicht möglich und nicht zielführend, sondern auch nicht rechtswissenschaftsadäquat und nicht sachlich.

Eine Reihe der genannten Evaluierungskriterien wirft die Frage nach ihrer Zweckmäßigkeit und Sachlichkeit auf. Ist es bspw zweckmäßig und sachlich, zur Messung der Verbreitung rechtswis-

76 Im Hinblick auf die Lehrfreiheit bereits *Smend* in VVDStRL 4, 68.
77 § 22 Abs 2 lit d Kollektivvertrag für die ArbeitnehmerInnen der Universitäten 2015.

senschaftlicher Forschungsleistungen auf Zitate oder Verweise in Gerichtsentscheidungen abzustellen? Eine einfache RIS-Abfrage macht dies möglich, soweit die Entscheidungen erfasst sind. Was sagt aber ein Zitat oder Verweis aus? Wohl nur, dass das Gericht seine Entscheidungsbegründung durch eine entsprechende Lehrmeinung abstützt; abweichende Auffassungen wird es dagegen kaum anführen. Was soll das aber nun genau über Qualität und Quantität der Forschungsleistung aussagen? Dieselbe Frage stellt sich bei Kriterien wie Arbeitszeit, Anwesenheit am Arbeitsplatz, PC-Laufzeit, Zahl einlangender und ausgehender Emails, aber auch Bibliotheksbesuche oder Häufigkeit der Inanspruchnahme elektronischer Kataloge, Suchmaschinen oder Datenbanken. Informationen dazu sind vorhanden, unabhängig davon, ob sie zur Evaluierung aus Datenschutzgründen überhaupt herangezogen werden dürfen. Sie demonstrieren aber nur Anwesenheit am Arbeitsplatz, Betrieb des PC, Kommunikation, Inanspruchnahme der Bibliothekseinrichtungen. Welche Aussagekraft haben sie aber hinsichtlich der Qualität und Quantität von Forschungsleistungen?

Unzulässig – weil wegen Verletzung der Wissenschaftsfreiheit verfassungswidrig – wäre es, wenn auf der Grundlage der Evaluierungsergebnisse, sei es, dass sie Forschungsleistungen abbilden, sei es, dass sie diese darüber hinaus auch qualitativ und/oder quantitativ bewerten, einem akademischen Forscher konkrete Forschungsverpflichtungen auferlegt werden, die die gesetzliche und kollektivvertragliche Forschungsverpflichtung näher bestimmen. In welcher Form – hoheitlich oder privatrechtlich – ein solcher, die wissenschaftliche Forschung durch ihre Lenkung beeinflussender Grundrechtseingriff erfolgt, ist zweitrangig, spielt diese doch nur bei der Durchsetzung der Wissenschaftsfreiheit im Konfliktfall eine Rolle.

So wäre es als ein unzulässiger Eingriff in die Wissenschaftsfreiheit zu qualifizieren, würde dem akademischen Forscher aufgetragen, in einem bestimmten Zeitraum eine bestimmte Anzahl von Publikationen zu verfassen, davon wiederum eine bestimmte Zahl fremdsprachige, in einem „höherwertigen“ Format erscheinende, in einer klassifizierten Zeitschrift zu veröffentlichende oder solche, die eine bestimmte wissenschaftliche oder gesellschaftliche „Relevanz“ aufweisen oder einem Forschungsschwerpunkt der Universität entsprechen, den wissenschaftlichen und/oder gesellschaftlichen „Impact“ seiner Forschungsergebnisse durch eine Erhöhung seiner Zitate oder Verweise durch Dritte zu erhöhen, häufiger auf wissenschaftlichen Konferenzen aufzutreten und dort vorzutragen oder Drittmittel in näher bestimmter Höhe einzuwerben. Ein unzulässiger Eingriff in die wissenschaftliche Forschung wäre auch anzunehmen, würde der akademische Forscher angehalten, seine Forschungstätigkeiten und -leistungen zu internationalisieren, wenn die vertretene Fachwissenschaft national bestimmt ist. Ebenso wäre es unzulässig, würde ihm im Zuge einer im Rahmen der Evaluierung erfolgenden qualitativen Bewertung der Forschungsleistungen gar nahegelegt, als methodisch nicht einwandfrei durchgeführt, unvertretbar, umstritten oder ethisch bedenklich erachtete Forschungsergebnisse zurückzunehmen. Von einem unzulässigen Eingriff müsste zudem ausgegangen werden, hätte die Nichterfüllung konkreter Forschungsverpflichtungen für den akademischen Forscher dienst- bzw arbeitsrechtliche Folgen, wie bspw die Kürzung des Gehaltes oder der ihm zur Verfügung gestellten finanziellen oder personellen Ressourcen.

Auch einer vertraglichen Übernahme konkreter Forschungsverpflichtungen durch den akademischen Forscher in seinem Dienstvertrag sind engste Grenzen gesetzt. Verpflichtet sich dieser im Zuge seiner Berufung zur Erbringung der Form nach bestimmter Forschungsleistungen in einem

bestimmten Zeitraum – bspw von zwei Monographien in einem längeren und jeweils drei weiteren Beiträgen und Vorträgen in kürzeren Zeiträumen und zur Antragstellung oder Erlangung der Bewilligung eines Drittmittelprojekts –, zu deren Evaluierung und dazu, dass er im Falle einer negativen Evaluierung einen Teil seines Gehaltes verliert, bewirkt diese vertragliche Vereinbarung eine von der Wissenschaftsfreiheit verpönte Lenkung wissenschaftlicher Forschung. Es ist dies zwar keine unmittelbare inhaltliche Lenkung, wohl aber eine durch Vorgabe der Publikations- und Verbreitungsform mittelbar erfolgende inhaltliche Steuerung.

Die Wissenschaftsfreiheit wird durch die vertragliche Vereinbarung nicht „ausgeschaltet". Es ist zwar richtig, dass der akademische Forscher über Privatautonomie verfügt, auch, dass er auf die Ausübung seiner Grundrechtspositionen verzichten kann.[78] Dies ist aber nur zulässig, wenn die Grundrechtsposition überwiegend privatnützig[79] ist, der Ausübungsverzicht freiwillig erfolgt und überdies nicht unverhältnismäßig ist.[80]

Dass die durch Art 17 Abs 1 StGG vermittelte Grundrechtsposition nicht überwiegend privatnützig ist, dass die „freie" Wissenschaft vielmehr insb auch dem öffentlichen Interesse dient, zeigen nicht nur die Entstehungsgeschichte der Wissenschaftsfreiheit,[81] sondern auch Art 81c B-VG[82] und § 2 Universitätsgesetz 2002[83]. Auch Freiwilligkeit wird bei Einwilligung in die wissenschaftsfreiheitbeschränkenden Vertragsbestandteile in der Regel nicht vorliegen: Die Zahl der Professuren ist beschränkt. Es gibt mehrere zu reihende Bewerber. Hinter dem Erstgereihten lauern der Zweit- und Drittgereihte. Der Erstgereihte steht unter Druck, er hat keine Verhandlungsmacht; er wird in die wissenschaftsfreiheitsbeschränkenden Vertragsbestandteile einwilligen, will er in seinem angestammten Fach an einer öffentlichen Universität tätig sein. Demnach wird regelmäßig ein Kräfteungleichgewicht zwischen den Vertragsparteien bestehen.

Ein solches Kräfteungleichgewicht bewirkt eine höhere Bindungsintensität der Schutzwirkungen der Wissenschaftsfreiheit: Vertragsbestimmungen, wie die in Rede stehende, werden daher als unverhältnismäßiger Eingriff, als Verletzung der Wissenschaftsfreiheit anzusehen sein, wenn der akademische Forscher dienst- bzw arbeitsrechtliche Konsequenzen bei Nichterreichung der vereinbarten Forschungsleistungen zu gewärtigen hat und er nicht vergleichbare Forschungsleistungen in beliebiger Publikations- und Verbreitungsform erbringen kann.

Demgegenüber begegnet eine Vertragsgestaltung, die Anreize zu besonderen, über den „*im Allgemeinen erzielbare[n] Arbeitserfolg*"[84] hinausgehenden wissenschaftlichen Forschungsleistungen

78 Zum Grundrechtsausübungsverzicht siehe *Merten*, Der Verlust von Grundrechten, in *Merten/Papier* (Hrsg), Handbuch der Grundrechte in Deutschland und Europa III (2009) § 73 Rz 24–74.

79 Siehe dazu auch *Merten* in *Merten/Papier* III § 73 Rz 37 mwN.

80 Siehe dazu grundlegend *Korinek/Holoubek*, Grundlagen staatlicher Privatwirtschaftsverwaltung (1993) 161; *Korinek/Holoubek*, Bundesverfassungsrechtliche Probleme privatrechtsförmiger Subventionsverwaltung (Teil Ia), ÖZW 1995, 1 und *Korinek/Holoubek*, Bundesverfassungsrechtliche Probleme privatrechtsförmiger Subventionsverwaltung (Teil II) ÖZW 1995, 108 (112).

81 „*[D]ie Wissenschaft sei nicht eine Domaine von Wenigen, wie Manche zu glauben scheinen, sondern ein Gemeingut des Volkes, und eines der wichtigsten; aber nur ihre Freiheit mache sie zu einem Gut*" so *Beseler* in *Droysen* 19.

82 Art 81c B-VG bezeichnet die öffentlichen Universitäten als „Stätten freier wissenschaftlicher Forschung, Lehre und Erschließung der Künste". Siehe bspw *Mayer/Muzak*, B-VG[5] Art 81c I.2. „*Die in [Art 81c] Abs 1 genannten Aufgaben, die von den öffentlichen Universitäten zu besorgen sind, sind ‚öffentliche Aufgaben'; als solche stehen sie im Dienste der Allgemeinheit*" und die Nachweise in FN 35.

83 Nach § 2 Z 1 und 3 UG sind insb die Freiheit der Wissenschaften und ihrer Lehre (Art 17 Abs 1 StGG) und die Vielfalt wissenschaftlicher Theorien, Methoden und Lehrmeinungen leitende Grundsätze für die öffentlichen Universitäten bei der Erfüllung ihrer Aufgaben.

84 Siehe FN 77

bietet und solche – freilich auf der Grundlage einer fachwissenschaftsadäquaten Evaluierung – in welcher Weise auch immer prämiert, keinen grundrechtlichen Bedenken.

Intrinsische Motivation und ein gesicherter Freiraum, in dem sich Wissenschaft entfalten kann, sind, wie *Georg Lienbacher* vor gut einem Jahr hier in Graz mit vollem Recht hervorgehoben hat, wohl die stärksten Anknüpfungspunkte für die Sicherung der Qualität (rechts)wissenschaftlicher Forschung. Diese liegen, wie die eingangs nachgezeichnete historische Entwicklung unmissverständlich zeigt, den Garantien der Wissenschaftsfreiheit zugrunde, sind für diese unabdingbar. Ihre Einschränkung in der soeben dargelegten Weise würde nicht nur verfassungswidriges Handeln bedeuten, sondern auch ein Zurückgehen hinter die mit der Wissenschaftsfreiheit im 19. Jahrhundert etablierten Errungenschaften.

Denn auch im 21. Jahrhundert mit seiner weitreichenden Technisierung und Digitalisierung des täglichen Lebens, mit den sich nunmehr für den akademischen Forscher bietenden Möglichkeiten digitaler Präsenz und digitaler Informationsbeschaffung, aber auch einer digital gestützten Evaluierung seiner Forschungsleistungen, die sein Profil – ja ihn selbst – zunehmend digitalisiert erscheinen lässt, ist – um mit den Worten von *Johann Gottlieb Fichte*[85] zu schließen – *„[d]er eigentlich belebende Odem der Universität, […] die himmlische Luft, in welcher alle Früchte derselben aufs fröhlichste sich entwickeln und gedeihen, […] ohne Zweifel*

die akademische Freiheit.“

85 *Fichte*, Ueber die einzig mögliche Störung der akademischen Freiheit – Eine Rede beim Antritte seines Rectorats an der Universität zu Berlin, den 19. 10. 1811 gehalten, in *Fichte* (Hrsg), Johann Gottlieb Fichte's sämmtliche Werke (1845) 450 (452).

AUSTRIAN LAW JOURNAL

ISSN: 2409-6911

DOI: 10.25364/1.4:2017.2.3
www.austrian-law-journal.at

Der digitalisierte Forscher

Stefan Storr[*], Universität Graz

***Kurztext**: Der vorliegende Kommentar bezieht sich auf den Beitrag „Der digitalisierte Forscher" von Thomas Kröll (ALJ 2/2017, 71). Ausgehend von der Beschreibung der gegenwärtigen Gesellschaft als Wissensgesellschaft werden drei Aspekte angeführt, die die Wissenschaft als System heute kennzeichnen und künftig weitere Bedeutung haben werden: die Gewinnung und Weitergabe von Forschungsdaten, die Bewertung von wissenschaftlichen Leistungen und die Funktion von Universitäten. Der Kommentar schließt mit der Aufforderung, das Grundrecht der Wissenschaftsfreiheit als institutionelle Garantie fortzuentwickeln.*

***Schlagworte:** Wissensgesellschaft, Wissenschaftsfreiheit, Digitalisierung, Text- und Data-Mining, Dissemination, Forschungsdaten, wissenschaftliche Leistungen, Bewertung, Ranking, Universitäten, Zugang zur IT-Kommunikationsinfrastruktur.*

I. Der Aufbruch in die Wissensgesellschaft

A. „Wissen ist Macht"

Das Thema „der digitalisierte Forscher" steht eng in Zusammenhang mit der Wissensgesellschaft. Die Wissensgesellschaft hat die Industriegesellschaft abgelöst. Während der industrielle Sektor zunehmend an Bedeutung verloren hat, ist ein Bedarf an hochqualifizierten Dienstleistungsberufen entstanden. Der amerikanische Soziologe *Daniel Bell* hat in seinem Werk *„The Coming of Post-Industrial Society"* schon 1973 das *„Primat des theoretischen Wissens"* hervorgehoben. Er hat erkannt, dass sich die nachindustrielle Gesellschaft zur *„sozialen Kontrolle und der Lenkung von Innovation und Wandel um Wissen"* organisiert.[1]

Dadurch bilden sich neue soziale Verhältnisse und neue Strukturen. *Bell* führt weiter aus: *„In dieser Gesellschaft treffen täglich Millionen Menschen Billionen von Entscheidungen – was sie kaufen, wie viele Kinder sie haben, wen sie wählen, welchen Beruf sie ausüben wollen usw. Dabei mag jede einzelne Entscheidung so unvorhersehbar sein wie die Reaktion eines Quantenatoms auf das Messinstrument, in der Summierung, der Gesamtheit jedoch lassen sie sich mit derselben Präzision bestimmen, mit der der Geometer seine Dreiecksmessungen durchführt. Wo der Computer der Diener ist, ist die Entscheidungstheorie der König."*[2] Damit ist das theoretische Wissen das strategische Instrument und das *„axiale Prinzip"* (*Bell*) der neuen Gesellschaft.

---

* Univ.-Prof. Dr. iur. *Stefan Storr* ist Dekan der Rechtswissenschaftlichen Fakultät sowie Universitätsprofessor am Institut für Öffentliches Recht und Politikwissenschaft der Karl-Franzens-Universität Graz.

1 *Bell*, Die nachindustrielle Gesellschaft[2] (1976) 36.

2 *Bell*, Gesellschaft[2] 49.

Fundstelle: *Storr*, Der digitalisierte Forscher, ALJ 2/2017, 85–94 (http://alj.uni-graz.at/index.php/alj/article/view/82).

Die Universitäten, Forschungsorganisationen und wissenschaftliche Institutionen sind die zentralen Schlüsselstellen dieser neuen Gesellschaft: Sie tragen das theoretische Wissen zusammen und werten es aus. Die Wissenschaftlerinnen und Wissenschaftler sind die Schlüssel der Wissensgesellschaft.

B. Die wissensbasierte Wirtschaft – die Lissabon-Strategie 2000

Die Wissensgesellschaft ist Realität: Der Europäische Rat hat in der Lissabon-Strategie 2000[3] die Herausforderungen einer neuen wissensbasierten Wirtschaft erkannt und den Aufbau von Wissensinfrastrukturen als *„klares strategisches Ziel"* definiert. Es sollte ein europäischer Forschungsraum geschaffen werden. Mit einem *„äußerst leistungsfähige[n] transeuropäischen Hochgeschwindigkeitsnetz für elektronische wissenschaftliche Mitteilungen"* sollten Forschungseinrichtungen und Universitäten sowie wissenschaftliche Bibliotheken, wissenschaftliche Zentren und, schrittweise, auch Schulen miteinander verbunden werden. Außerdem sollten sich Europas Bildungs- und Ausbildungssysteme auf den Bedarf der Wissensgesellschaft einstellen und es sollte einen breiteren Zugang zum Wissen geben. Die Europäische Union sollte die wettbewerbsfähigste und dynamischste Wissensgesellschaft der Welt werden.

C. Die Digitalisierung als das technische Rückgrat der Wissensgesellschaft

Die Digitalisierung ist das technische Rückgrat der Wissensgesellschaft. Die Digitalisierung von Daten und die moderne Kommunikationsinfrastruktur ermöglichen die Bereitstellung, die Suche, den sehr schnellen Transport und die Verarbeitung einer großen Masse an Daten.

Sie erlaubt die Speicherung von großen Datenmengen auch auf anderen Computern (Cloudcomputing), sogar die Nutzung fremder Computer.[4] Sie ermöglicht den Umgang mit Masseninformationen und ist die technische Grundlage für die Einbeziehung einer Vielzahl von Akteuren. Erst durch die Digitalisierung können leistungsfähige Forschernetzwerke entstehen, länderübergreifend, gar global zusammenarbeiten, Daten gewinnen und austauschen.

Die Digitalisierung ist die technische Voraussetzung, um Informationen als Steuerungsmittel intensiv einsetzen zu können. In der Tat übt der moderne Staat seine Hoheitsgewalt nicht mehr nur durch Regeln, Zwang und ökonomische Kompetenz aus, sondern auch durch Informationen, die er zunächst sammelt, auswertet und dann durch Aufklärung, Warnung und Empfehlung veröffentlicht, wodurch er Steuerungsergebnisse erzielt, die er durch Gebote und Verbote nicht erzielen würde.[5]

Es gibt noch viele weitere Phänomene. Fest steht: Die Digitalisierung und gesellschaftliche, wirtschaftliche und wissenschaftliche Entwicklungen aufgrund der Digitalisierung ändern unser Umfeld und uns in vielerlei Hinsicht. Was den digitalisierten Forscher selbst betrifft, ist seine Welt nicht nur die der Wissenschaft, auch andere Lebenssphären sind durch Digitalisierung im Wandel

3 *Europäischer Rat*, 23. und 24. 3. 2000 in Lissabon – Schlussfolgerungen des Vorsitzes.

4 Ein berühmtes Beispiel ist die Nutzung von privaten Computern im Rahmen des SETI@Home-Projekts (Berkley) zur Suche nach Radiosignalen von Außerirdischen. Ferner: Folding@home-Projekt (Stanford) zur Berechnung der Proteinfaltung oder das Cancer Research Project (Oxford) zur Untersuchung von Proteinen, die im Verdacht stehen, Auslöser für Krebs zu sein.

5 *Pöschl*, Sicherung grund- und menschenrechtlicher Standards gegenüber neuen Gefährdungen durch private und ausländische Akteure, VVDStRL 74 (2015) 405 (420).

begriffen und er betritt zB auch als Arbeitnehmer und als Privatperson das „Zeitalter der Digitalisierung".

Die rechtswissenschaftliche Forschung hat bereits begonnen, Bedeutung und Auswirkung der Digitalisierung in den einzelnen Teilrechtsgebieten zu verfolgen: Im Zivilrecht etwa werden Fragen zu Verträgen über digitale Inhalte oder die Haftung bei Inanspruchnahme unentgeltlicher Leistungen im Internetabschluss aufgearbeitet,[6] im Arbeitsrecht stellen sich Fragen des Arbeitszeit- und Urlaubsrechts, des Schutzes vor psychischen Belastungen, des technischen Arbeitsschutzes oder ganz das „Recht auf Nichterreichbarkeit",[7] ferner des Urheberrechts.[8] Das IT-Recht hat sich als eigenes Rechtsgebiet bereits etabliert.

Im Weiteren sollen drei Aspekte herausgegriffen werden, die die Welt des digitalisierten Forschers in ganz unterschiedlichen Zusammenhängen betreffen.

II. Gewinnung und Weitergabe von Forschungsdaten

A. Die Gewinnung von Daten

Text- und Data-Mining[9] sind neue Techniken, die es ermöglichen, Informationen, die in digitalisierter Form vorliegen, automatisch auszuwerten. Sie sind eine wesentliche Voraussetzung, um mit Big Data umgehen zu können, also massenhaft vorliegenden Daten, mit denen *„volume"* (Datenvolumen), *„velocity"* (Geschwindigkeit der Gewinnung und Verarbeitung von Daten) und *„variety"* (Bandbreite der Datentypen) verbunden werden. Text- und Data-Mining hat viele Anwendungsmöglichkeiten in der Wirtschaft, aber auch in der Forschung, zB für die gentechnische und biometrische Forschung.[10]

Rechtlich ist das Sammeln von Daten zunächst unter den Gesichtspunkten des Datenschutzes und des Urheberechts von Bedeutung. Wenn die Daten urheberrechtlich geschützt sind oder personenbezogene Daten enthalten, bedarf ihre Verarbeitung entweder einer gesetzlichen Grundlage oder einer Einwilligung des Betroffenen. Gerade die Einwilligung wird bei Big Data nur schwer für eine Vielzahl von Personen erlangt werden können. Das Ersuchen um Einwilligung muss *„in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache"* erfolgen und zwar so, *„dass es von den anderen Sachverhalten klar zu unterscheiden ist"*. Implizite Einwilligungen durch vorgegebene Erklärungen in Allgemeinen Geschäftsbedingungen sind damit nicht zulässig, sondern müssen ausdrücklich abgegeben werden.[11]

6 ZB *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update? Gutachten zum 71. Deutschen Juristentag (2016) A 9 ff.

7 *Krause*, Digitalisierung der Arbeitswelt – Herausforderungen und Regelungsbedarf, Gutachten zum 71. Deutschen Juristentag (2016) B 1 ff; *Oetker*, Digitalisierung der Arbeitswelt – Herausforderungen und Regelungsbedarf, JZ 2016, 817 ff.

8 *Ohly*, Urheberrecht in der digitalen Welt – Brauchen wir neue Regelungen zum Urheberrecht und dessen Durchsetzung? Gutachten zum 70. Deutschen Juristentag (2014) F 1 ff; *Leistner*, Urheberrecht in der digitalen Welt, JZ 2014, 846 ff.

9 Legaldefinition in Art 2 Abs 2 Vorschlag für eine Richtlinie über das Urheberrecht im digitalen Binnenmarkt vom 14. 9. 2016, COM(2016) 593 final.

10 Vgl auch COM(2016) 593 final.

11 *Spindler*, Big Data und Forschung mit Gesundheitsdaten in der gesetzlichen Krankenversicherung, MedR 2016, 691 (698).

Nicht selten stellt sich außerdem heraus, dass einmal erhobene und verwendete Daten später zu einem anderen Zweck verwendet werden sollen. Der Grundsatz der Zweckbindung ist eine wesentliche Festlegung des Datenschutzrechts.

Deshalb sind bestimmte Privilegien für die Wissenschaft wichtig: Die EU-DSGVO enthält eine wichtige Ausnahme für *„eine Weiterverarbeitung […] für wissenschaftliche oder historische Forschungszwecke"*. Sie gelten nicht als *„unvereinbar mit den ursprünglichen Zwecken"*.[12]

Außerdem entfällt die Speicherbegrenzung für personenbezogene Daten, soweit diese *„für wissenschaftliche […] Forschungszwecke […]"* erfolgt und technische und organisatorische Maßnahmen bestehen, mit denen insb die Achtung des Grundsatzes der Datenminimierung gewährleistet wird.[13] Dann sind auch die Informationspflichten gegenüber den Betroffenen und das Recht auf Löschung relativiert.[14]

Wichtig erscheint ferner der Vorschlag der Kommission zum Urheberrecht im digitalen Binnenmarkt, Data-Mining für Forschungsorganisationen grds zu vereinfachen und die Mitgliedstaaten zu verpflichten, Ausnahmen für Vervielfältigung und Entnahmen einzuführen, *„die durch Forschungsorganisationen von Werken oder sonstigen Schutzgegenständen, zu denen sie für die Zwecke der wissenschaftlichen Forschung rechtmäßig Zugang haben, für das Text- und Data-Mining vorgenommen wurden"*.[15]

B. Dissemination

Das bedeutsamste Medium für eine Dissemination von Forschungsergebnissen auf digitalem Wege ist das Internet. Wissenschaftliche Kommunikation kann zB durch E-Email, mithilfe von Suchmaschinen, Online-Zeitschriften, Digitale Bibliotheken oder Wissenschaftsblogs erfolgen.[16]

Es liegt nahe, dass die Breite des Informationsangebots, die durch Digitalisierung ermöglicht wird, einerseits zu einer starken Spezialisierung vieler Online-Medien führen wird; andererseits wird sich die Schnelligkeit des Datenzugriffs und der Datenverarbeitung auf die Geschwindigkeit, mit der neue Forschungsergebnisse gewonnen werden, auswirken. Dies wiederum zieht die Erwartungen der Forscher nach sich, dass ihre Forschungsergebnisse möglichst schnell für den relevanten Adressatenkreis publiziert werden.[17]

Printverlage haben ihre Angebote längst erweitert und stellen Datenbanken zur Verfügung, deren Zugang zumeist kostenpflichtig ist, wobei die Preise so ausgestaltet sind, dass die Leser an die Angebote des Verlages gebunden werden. Obwohl das Unterhalten einer Datenbank relativ kos-

12 Art 5 Abs 1 lit b VO (EU) 679/2016 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 2016/119, 1.

13 Art 5 Abs 1 lit e VO (EU) 679/2016 ABl L 2016/119, 1.

14 Art 14 Abs 5 lit b und Art 17 Abs 3 lit d VO (EU) 679/2016 ABl L 2016/119, 1.

15 Art 3 COM(2016) 593 final.

16 In Anlehnung an *Vowe*, Wissenschaftskommunikation 2.0? Fachzeitschriften in der Online-Welt, Publizistik 2016, 51 (57 f): Foren und Netzwerke für Wissenschaftler (wie ResearchGate), Enzyklopädien (wie Wikipedia), Wissensmanagementsysteme (wie Wolfram Alpha), Online-Verlagsangebote (wie SpringerLink), Websites etablierter und nicht-etablierter Organisationen, Intranets, Wissenschaftsjournalismus, Marktplätze für Personal, Finanzierung und Geräte (wie academics.de), Newsletter (wie von der EU), Datenarchive (Clouds), Plattformen für Data Sharing, Instrumente für Online-Datenerhebung, Online-Programme für vernetztes Arbeiten.

17 *Vowe*, Publizistik 2016, 62.

tengünstig erfolgen kann, wird damit die Marktstellung eines Onlinemediums zu einem wesentlichen Faktor für seine Attraktivität bei Autoren, in diesen zu publizieren.

Es gibt aber auch ein großes Interesse, Forschungsergebnisse möglichst breit (am besten der Allgemeinheit) und möglichst kostengünstig (am besten kostenlos) zu veröffentlichen. Open Access wird von den Wissenschaftsinstitutionen zB im Rahmen der Förderbedingungen eingefordert, die zB eine Dissemination der von ihnen geförderten Forschung in nicht zugangsbeschränkten Medien verlangen.

Für die Wissenschaft von besonderer Bedeutung erscheinen zwei weitere im Urhebergesetz geregelte Privilegien, die eine Verbreitung urheberrechtlich geschützter Werke ausnahmsweise ermöglichen: Einmal das Zweitverwertungsrecht nach § 37a UrhG für Urheber eines wissenschaftlichen Beitrags. Wenn der Urheber dem Verleger oder Herausgeber ein Werknutzungsrecht eingeräumt hat, darf er dennoch sein Werk zweitveröffentlichen. Dieses Recht besteht ua erst nach Ablauf von zwölf Monaten seit der Erstveröffentlichung. Die Zweitveröffentlichung darf keinem gewerblichen Zweck dienen. Der Urheber muss Angehöriger des wissenschaftlichen Personals einer mindestens zur Hälfte mit öffentlichen Mitteln finanzierten Forschungseinrichtung sein und der Beitrag muss in einer periodisch mindestens zweimal jährlich erscheinenden Sammlung erschienen sein.

Außerdem ist die Vervielfältigung eines wesentlichen Teils einer veröffentlichten Datenbank zu Zwecken der Wissenschaft zulässig. Die Vervielfältigung darf nur in einem durch den Zweck gerechtfertigten Umfang erfolgen und es darf kein Erwerbszweck verfolgt werden (§ 76d Abs 3 S 2 UrhG[18]).

III. Die „Statistikgläubigkeit“

A. Die Bewertung von wissenschaftlichen Leistungen der Forscherinnen und Forscher

In der „Statistikgläubigkeit“ kann eine erhebliche Gefährdung der Wissenschaftsfreiheit liegen. In den vergangenen Jahren hat diese im Zuge der Einführung von Methoden des New Public Managements und der diese begleitenden Formen des Wissenschaftscontrollings Einzug in die Universitäten gehalten.

Schon grundsätzlich ist es die Wissenschaftlichkeit einer Leistung selbst, die einer Beurteilung nach statistischen Maßstäben entgegensteht. Obwohl der VfGH den Schutzgehalt der Wissenschafts- und Forschungsfreiheit erst zu Teilen konturiert hat,[19] gilt im Schrifttum doch als allgemein akzeptiert, dass wissenschaftliche Forschung jedenfalls die Suche nach neuen Erkenntnissen unter Heranziehung wissenschaftlicher Methoden ist,[20] wobei der Wissenschaftsbegriff in hohem Maße vom Selbstverständnis der *scientific community* über das, was wissenschaftlich ist, geprägt wird.

Das erhellt, dass einem Bemühen, mit statistischen Auswertungen von wissenschaftlichen Tätigkeiten und Leistungen eine Bewertung vorzunehmen, mit höchster Vorsicht zu begegnen ist.

18 Vgl Art 6 Abs 2 lit b und 9 lit b Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken, ABl L 1996/77, 20.

19 Siehe nur VfSlg 3191/1957.

20 *Kröll* in *Kneihs/Lienbacher* (Hrsg), Rill-Schäffer-Kommentar zum Bundesverfassungsrecht (13. Lfg 2014) Art 17 Abs 1, 5 StGG Rz 30.

Zumeist ist die Statistik nämlich nur ein Ersatzmaßstab, mit dem weder die Wissenschaftlichkeit einer Tätigkeit noch die Bedeutung eines Ergebnisses dieser Tätigkeit beurteilt werden kann.

Mit einer Statistik zB wie viele (wissenschaftliche) Beiträge in bestimmten Fachzeitschriften veröffentlicht oder welche und wie viele Drittmittel eingeworben wurden, kann nur dahingehend eine Aussage getroffen werden, dass bestimmte wissenschaftliche Einrichtungen wie Herausgeber von Fachzeitschriften und drittmittelgebende Förderstellen, Beiträge eines bestimmten Wissenschaftlers oder einer Wissenschaftlerin angenommen oder gefördert haben. Das lässt einen Schluss dahingehend zu, dass diese Einrichtungen davon ausgehen, dass sich ein bestimmter Wissenschaftler oder eine Wissenschaftlerin wissenschaftlich betätigt hat; über die Bedeutung dieser Wissenschaft bzw des Ergebnisses ist damit aber nichts gesagt.

B. Die Bedeutung wissenschaftlicher Leistung für das Hochschulbudget

Obwohl Statistiken in vielen Fällen keine Aussage zur Quantität und Qualität wissenschaftlicher Forschung zulassen, werden sie dennoch als wissenschaftsrelevante „Pseudo-Aussagen" als Grundlage für Entscheidungen herangezogen.

Das Globalbudget österreichischer Hochschulen setzt sich unter anderem aus den Hochschulraum-Strukturmittel zusammen, die anhand von *„qualitäts-, quantitäts- und leistungsbezogenen Indikatoren bemessen"* werden sollen. Diese beziehen sich unter anderem auf den Bereich Forschung.[21] Die Hochschulraum-Strukturmittelverordnung (HRSMV) benennt in § 3 forschungsbezogene Indikatoren. Sie kennt zwar in § 2 Abs 2 nur fünf Teilbeträge, wobei der Teilbetrag für Wissenstransfer (15 %) und der für strukturierte Doktoratsausbildungen (4 %) den Bereich Forschung betreffen, jedoch soll der Teilbetrag Wissenstransfer nach § 3 Abs 2 lit c durch den sog *„Indikator III: ‚Erlöse aus F&E-Projekten/Projekten der Entwicklung und Erschließung der Künste in Euro'"* bestimmt werden. Nach § 6 Abs 1 sollen dafür ausschließlich Erlöse berücksichtigt werden, die von der EU und vom FWF lukriert werden, wobei Erlöse, die vom FWF lukriert werden, mit dem Faktor 2 gewichtet werden. Wenngleich wissenschaftliche Aussagen nicht direkt bewertet werden, sondern nur in ihrer Gesamtheit, und ihnen auch nur Budgetrelevanz zukommen soll, kann die Sachlichkeit dieses Maßstabs nicht nachvollzogen werden, denn die Konzentration des Indikators auf EU- und FWF-Drittmittel sowie die höhere Gewichtung von FWF-Drittmitteln lassen eine Aussage über die Wissenschaftlichkeit dieser oder anderer Tätigkeiten nicht zu.

Detaillierter ist die Wissensbilanz-Verordnung (WBV),[22] die allerdings nicht unmittelbar budgetrelevant ist. Nach §§ 3, 4 Abs 2 Z 2 sind in einem Leistungsbericht der Output der Forschung und Entwicklung wie zB wissenschaftliche Publikationen bzw Leistungen oder wissenschaftliche Veranstaltungen anzugeben. In einer Statistik mögen diese Angaben übersichtlich zusammengefasst und präsentiert werden können; um die Wissenschaftlichkeit der Tätigkeiten zu beurteilen sind sie nicht geeignet.

21 § 2 Abs 1 Verordnung des Bundesministers für Wissenschaft und Forschung über die Bemessung der Hochschulraum-Strukturmittel (Hochschulraum-Strukturmittelverordnung – HRSMV) BGBl II 2012/292 idF BGBl II 2016/97.

22 Verordnung des Bundesministers für Wissenschaft, Forschung und Wirtschaft über die Wissensbilanz (Wissensbilanz-Verordnung-2016 – WBV 2016) BGBl II 2016/97 idF BGBl II 2017/69.

C. Ranking von Hochschulen

Auf der Grundlage einer Fülle von Daten werden auch Hochschulen bewertet und zueinander in Beziehung gesetzt. Allerdings sind diese Bewertungen sehr subjektiv. Zum einen weil die Datenqualität sehr unterschiedlich ist, zum anderen weil bei internationalen Hochschulrankings nationale Rahmenbedingungen (zB offener Hochschulzugang in Österreich, Diplomstudiengang Jus…) häufig keine Rücksicht finden. Auch die unterschiedlichen Wissenschaftskulturen werden nicht immer hinreichend abgebildet und auf Besonderheiten einzelner Hochschulen wird keine Rücksicht genommen.[23] Schließlich werden die Indikatoren je nach subjektiver Einschätzung verschieden stark gewichtet. Nicht zuletzt gibt es sehr viele Rankings (derzeit mehr als 20).[24]

Obwohl diese Kritik ganz überwiegend geteilt wird und die Aussagekraft in Frage gestellt wird, werden die Bewertungen dennoch vorgenommen und daraus Schlüsse gezogen. Die Hochschul-Rankings finden international hohe Beachtung, gelten als „Qualitätssiegel" und als Orientierungshilfe. Der Grund dürfte in der Einfachheit der Aussage liegen, die die Statistik bietet. Während aus einer großen Menge an Daten nur sehr schwer eine Gesamtbewertung ohne Verarbeitung und Auswertung der Daten möglich ist und jede Differenzierung die Komplexität erhöht, bietet das Ranking eine einfache und klare Botschaft. Dass diese zu einfach ist und deshalb zu kurz greift bzw die Schlussfolgerungen falsch sind, scheint kaum Gehör zu finden. Es ist bemerkenswert, dass die Uniko das Hochschulranking einerseits sehr kritisch sieht – dies wohl deshalb, weil ihre Mitglieder im internationalen Vergleich nicht so reüssieren können wie erhofft wird – andererseits sind es die Universitäten selbst, die an der Statistik zur Messung von einzelnen Leistungen ihrer Mitarbeiter festhalten.

IV. Die Rolle der Universitäten

In der Wissensgesellschaft kommt den Universitäten eine zentrale Rolle zu. Sie sind die Institutionen, die Wissenschaft ermöglichen, die die erforderlichen Daten oder den Zugang zu diesen Daten herstellen, die die Infrastruktur für die Auswertung dieser Daten bereitstellen. Sie beschäftigen Wissenschaftlerinnen und Wissenschaftler und geben ihnen die Möglichkeit für Forschung sowie die Teilnahme am wissenschaftlichen Diskurs und sind die Institutionen, die Wissenschaft in die Lehre einfließen lassen können. Die Universitäten sind – zusammen mit anderen Forschungseinrichtungen – die wichtigsten Akteure und Proponenten der Wissensgesellschaft.

Es liegt nahe, die Wissenschaft als System im *Luhmannschen* Sinne[25] anzuführen, das nach eigenen Prinzipen und Regeln funktioniert. Diese (große) Gemeinschaft der Wissenschaftlerinnen und Wissenschaftler ist damit – um erneut auf *Bell* zurückzugreifen – die *„Republik freier, durch die gemeinsame Suche nach der Wahrheit vereinter Männer und Frauen"*, die dem *„Ideal der griechischen Polis"* entspricht,[26] sozusagen die *„Republic of Science"*.[27]

Die Gemeinschaft der Wissenschaftlerinnen und Wissenschaftler stand bisher auf zwei Säulen: Der Freiheit der Wissenschaft und der Autonomie der Universitäten. Mit der Digitalisierung

23 *Österreichische Universitätenkonferenz (Uniko)*, Internationale Hochschulrankings und ihre Bedeutung für die österreichischen Universitäten (2017) 5.
24 *Uniko*, Hochschulrankings, 8.
25 *Luhmann*, Die Wissenschaft der Gesellschaft (1990) 271 ff.
26 *Bell*, Gesellschaft[2] 278.
27 *Wielsch*, Die epistemische Analyse des Rechts, JZ 2009, 67.

kommt aber eine dritte Säule hinzu: Die Zurverfügungstellung von Kommunikationsinfrastruktur. Wer keinen Zugang zur Kommunikationsinfrastruktur hat, ist von der Gemeinschaft der Wissenschaftlerinnen und Wissenschaftler ausgeschlossen.

V. Aktuelle Anforderungen an das Grundrecht der Wissenschaftsfreiheit

Angesichts der dargestellten Entwicklungen ist es erforderlich, das Grundrecht der Wissenschaftsfreiheit dogmatisch fortzuentwickeln. Art 17 StGG, der auf die Märzverfassung 1849 zurückgeht,[28] ist 1867 in Kraft getreten und hatte zwei Zielrichtungen: Den Schutz gegen polizeistaatliche Beeinflussung, wie sie im Vormärz vorkam, und den Schutz gegen Einflussnahmen der Kirche, wie sie in der Mitte des 19. Jahrhunderts erfolgte.[29] Der VfGH hat im UOG-Erkenntnis (1977) das Grundrecht der Wissenschaftsfreiheit in Art 17 StGG noch sehr eng ausgelegt und im Lichte des Entstehungsprozesses 1867 als bloßes Abwehrrecht interpretiert, das nur vor intentionalen Eingriffen des Staates schütze.[30] Obwohl das Grundrecht keinen Gesetzesvorbehalt kennt, besteht Übereinstimmung dahingehend, dass der grundrechtliche Schutz einem immanenten Schrankenvorbehalt unterliegt und seine Grenzen in den Grundrechten Dritter und anderen gemeinwohlorientierten Zielen findet.[31] Dennoch soll das Grundrecht der Wissenschaftsfreiheit nach VfGH nur ein Sonderfall des Rechts der freien Meinungsäußerung und dem Grundrecht der Kunstfreiheit ähnlich sein,[32] aber *„keinerlei ‚institutionellen Bezug'"* haben.[33]

Richtig ist, dass der Umgang mit Wissen in verschiedener Hinsicht grundrechtlich abgesichert ist, wobei Meinungsfreiheit (Art 10 EMRK, Art 11 GRC), Datenschutz (zB Art 8 GRC) bzw Privatheit (zB Art 7 GRC) und Informationsfreiheit (Art 11 GRC) wesentliche Eckpfeiler sind. Aber die vom VfGH formulierte Stoßrichtung der Wissenschaftsfreiheit kann die heutigen Gefährdungen angesichts der voranschreitenden Digitalisierung und der damit verbundenen Internationalisierung und Organisation der Universitäten nicht mehr effektiv abwehren. Vielmehr muss das Grundrecht als eine institutionelle Garantie begriffen werden, aus der eine Gewährleistungsverpflichtung des Staates und seiner Einrichtungen folgt, die Wissenschaft von fremdbestimmten Einflüssen möglichst frei zu halten[34] und Wissenschaft zu ermöglichen. Das Grundrecht der Wissenschaftsfreiheit ist als Teilhabegrundrecht fortzuentwickeln.

A. Die wissenschaftsadäquate Beurteilung und Bewertung wissenschaftlicher Leistungen

Das betrifft einmal die wissenschaftsadäquate Beurteilung und Bewertung wissenschaftlicher Leistungen. Die dahingehende Verpflichtung ist eine materielle, dh sie gilt auch für staatliche Universitäten als *„Stätten freier wissenschaftlicher Forschung"* iSd Art 81c B-VG. Die Universitäten bzw ihre Verwaltungen dürfen wissenschaftliche Tätigkeiten zwar statistisch messen; auf ihren

28 *Kröll*, Der digitalisiert Forscher, ALJ 2017, 71.
29 *Kröll* in *Kneihs/Lienbacher* Art 17 Abs 1, 5 StGG Rz 20.
30 VfSlg 8136/1977.
31 *Berka*, Verfassungsrecht[6] (2016) 452.
32 VfSlg 13978/1994.
33 VfSlg 8136/1977.
34 *Mayer/Kucsko-Stadlmayer/Stöger*, Bundesverfassungsrecht[11] (2015); allgemein, insb auch zur institutionellen Garantie siehe *Kröll* in *Kneihs/Lienbacher* Art 17 Abs 1, 5 StGG Rz 92; *Pöschl*, Von der Forschungsethik zum Forschungsrecht: Wieviel Regulierung verträgt die Forschungsfreiheit, in *Körtner/Kopetzki/Druml* (Hrsg), Ethik und Recht in der Humanforschung (2010) 90 (116).

wissenschaftlichen Gehalt hin beurteilen können sie diese aber nur unter Zugrundelegung der Methoden, die im jeweiligen wissenschaftlichen Fach als wissenschaftliche anerkannt sind. Aus statistischen Erhebungen gar aus statistischen Vergleichen mit anderen wissenschaftlichen Fächern können jedenfalls keine wissenschaftlichen Ergebnisse gewonnen werden.

B. Zugang zur IT-Kommunikationsinfrastruktur

Unbestritten umfasst das Grundrecht der Wissenschaftsfreiheit das Recht der Verbreitung der eigenen Forschungsergebnisse.[35] Das schließt das Recht, das Publikationsmedium zu wählen, ein. Damit eröffnet die Digitalisierung dem Forscher erhebliche Möglichkeiten der Dissemination insb über das Internet. Umgekehrt ist die Verpflichtung eines Wissenschaftlers, Forschungsergebnisse nicht zu publizieren oder Forschungsergebnisse publizieren zu müssen, nur abgeändert zu veröffentlichen oder Publikationen zurückzuziehen ein Grundrechtseingriff.[36]

Im Zeitalter der Digitalisierung ist der Zugang zu Datenbanken, wie überhaupt der Zugang zur IT-Kommunikationsinfrastruktur, grundlegend geworden: Zum einen, weil sie einen Zugriff auf Daten erlaubt und eine Verbreitung ermöglicht, zum anderen weil Wissenschaft fast nur noch mit digitaler Infrastruktur erfolgt. Mit anderen Worten ist derjenige vom Wissenschaftsbetrieb ausgeschlossen und wird von Möglichkeiten der Datengewinnung und Verbreitung sowie der Möglichkeit, seine Forschungsbeiträge in den wissenschaftlichen Diskurs einzuführen, abgeschnitten, dem dieser Zugang nicht gewährt wird. In der Wissensgesellschaft muss das Grundrecht der Wissenschaftsfreiheit deshalb auch ein Teilhaberecht gewährleisten.

Das heißt nicht, dass dem einzelnen Wissenschaftler ein grundrechtlich gewährtes Recht auf umfassenden Zugang zukommen kann. Zwar kann es für den Erfolg eines wissenschaftlichen Beitrags von großer Bedeutung sein, diesen in einer bzw einer bestimmten Datenbank unterzubringen. Doch wird eine Grundrechtsdogmatik der Wissenschaftsfreiheit, die einen Zugang zu einer (bestimmten) Datenbank verspricht, sei diese privat oder staatlich geführt, schon deshalb nicht hergeleitet werden können, weil dem Wissenschaftler ja nicht jede Form der Dissemination verschlossen wird und jedenfalls der allgemeine Internetzugang möglich ist.

Eine weitere Frage ist, ob aus Art 17 StGG der Staat, zB eine staatliche Universität, verpflichtet sein kann, Internetzugang bzw Zugang zu einer bestimmten oder mehreren Datenbanken zur Verfügung zu stellen. Dann geht es letztlich um die Zurverfügungstellung von Ressourcen, betrifft also eine Teilhabekonstellation, die grundrechtsdogmatisch restriktiv zu behandeln ist. Selbst das deutsche BVerfG, das eine prospektive Grundrechtsdogmatik verfolgt, leitet aus dem Grundrecht der Wissenschaftsfreiheit des Art 5 Abs 3 GG zwar die Verpflichtung der Universitätsorgane ab, bei der Verteilung der verfügbaren Mittel jedenfalls die Personal- und Sachmittel zuzuweisen, die es überhaupt erst ermöglichen, wissenschaftliche Forschung und Lehre zu betreiben,[37] hat diese Mindestanforderung aber nie spezifiziert. Wenn es aber zutrifft, dass Universitäten in der Wissensgesellschaft die zentralen wissenschaftlichen Institutionen sind, werden ihnen auch grundsätzliche Verpflichtungen zur Verfügungstellung und Gewährleistung eines ausreichenden Angebots an IT-Kommunikationsinfrastruktur obliegen müssen. Das Grundrecht der Wissenschafts-

35 *Hengstschläger/Leeb*, Grundrechte[2] (2013) 236.
36 *Pöschl* in *Körtner/Kopetzki/Druml* 121.
37 BVerfGE 111, 333 (362) (Brandenburgisches Hochschulgesetz).

freiheit bedarf einer dogmatischen Fortbildung zu einem Recht, sich wissenschaftlich betätigen zu können, was im Zeitalter der Digitalisierung einen Zugang zur Kommunikationsinfrastruktur einschließt.[38] Gestützt wird dieses Anliegen durch den Internationalen Pakt über wirtschaftliche, soziale und kulturelle Rechte, mit dem sich die vertragsschließenden Staaten verpflichtet haben, das Recht eines jeden anzuerkennen, an den Errungenschaften des wissenschaftlichen Fortschritts und seiner Anwendung teilzuhaben.[39]

Möglicherweise könnte das in der GRC kodifizierte Grundrecht der Wissenschaftsfreiheit (Art 13 GRC) neue Impulse für die Wissenschaft in der Wissensgesellschaft setzen. Es liegt nahe, dass internationalen Vereinbarungen und Gewährleistungen angesichts der Internationalisierung, die durch die Digitalisierung wesentlich erleichtert und gefördert wird, Bedeutung zukommen wird. Jedoch hat Art 13 GRC bisher kaum wissenschaftliche Beachtung gefunden; auch der EuGH hat bisher keinen Bedarf gesehen, auf diese Grundrechtsgewährleistung zuzugreifen.[40]

38 Zur Kommunikationsermöglichung allgemein: *Cornils*, Entterritorialisierung im Kommunikationsrecht, VVDStRL 76 (2017) 391 (432).

39 Art 15 Abs 1 lit b Internationaler Pakt über wirtschaftliche, soziale und kulturelle Rechte BGBl 1978/590 idF BGBl III 2016/224; allerdings unter dem Vorbehalt des Art 2 Abs 1: unter Ausschöpfung der Möglichkeiten des betreffenden Staats und nur *„nach und nach mit allen geeigneten Mitteln, vor allem durch gesetzgeberische Maßnahmen“*.

40 Im Grundrechtekonvent war der Freiheit der Wissenschaft wenig Aufmerksamkeit zu Teil geworden: *Bernsdorff* in *Meyer* (Hrsg), Charta der Grundrechte der Europäischen Union[4] (2014) Art 13 Rz 6.

AUSTRIAN LAW JOURNAL

ISSN: 2409-6911

DOI: 10.25364/1.4:2017.2.4
www.austrian-law-journal.at

Datenschutz in den sozialen Medien aus privatrechtlicher Perspektive

Johannes Hager*, Universität München

***Kurztext**: Der Datenschutz in den sozialen Medien wirft eine Reihe von Problemen auf. Zum einen geht es um das Verhältnis des Datenschutzgesetzes zum Persönlichkeitsrecht; hier wird sich eine Kombinationslehre wie bei sonstigen besonderen Persönlichkeitsrechten – etwa dem Bildnisschutz – als überlegen erweisen. Die §§ 7 ff dTMG privilegieren die Provider in mehrfacher Hinsicht. Freilich bleibt deren Haftung oft unberührt. So kann der Content-Provider zur Verantwortung gezogen werden auch wenn er sich fremde Nachrichten nur zu eigen macht. Der Host-Provider haftet ab Kenntnis des rechtswidrigen Inhalts; auch treffen ihn eine Reihe von Prüfungspflichten. Entgegen der Auffassung des BGH ist er auch verpflichtet, den Namen des Content-Providers zu nennen. Schließlich kommt eine Haftung des Access-Providers in Betracht, wenn er die rechtswidrigen Inhalte wissentlich weiterleitet. Entgegen der Auffassung des EuGH besteht ein Gerichtsstand überall dort, wo sich die unerlaubte Handlung – die Verletzung des Persönlichkeitsrechts – verwirklicht; sie ist nicht auf den Tatort und den Ort beschränkt, an dem sich das Opfer befindet.*

***Schlagworte:** Datenschutz, Persönlichkeitsrecht, Gerichtsstand, Access-Provider, Content-Provider, Host-Provider.*

I. Einleitung

Die sozialen Netzwerke haben in den letzten Jahren eine ungeahnte Entwicklung genommen. Im 4. Quartal 2016 hatte Facebook nach eigenen Angaben 1,86 Mrd Nutzer; einen belastbaren Beleg dafür gibt es allerdings nicht.[1] Entsprechend groß ist auch das Potenzial der Schädigungsmöglichkeit der Mitglieder. Ein Beispiel ist der Fall des syrischen Flüchtlings Anas *Modamani*, der – bekannt geworden durch das Foto mit der Kanzlerin Angela *Merkel* – sich in Facebook der Kampagne ausgesetzt sieht, er habe an schwersten Straftaten mitgewirkt, wie etwa dem Terroranschlag in Brüssel.[2] Die Verteidigung von Facebook ist eher matt. Es sei schwierig, die Löschung vorzunehmen; ein Argument, das angesichts eines Nettoertrags – nach Steuern – von 10,217 Mrd Dollar[3] doch etwas verwundert. Das zweite Argument wirkt noch erstaunlicher. Man verfüge nicht über die spezielle Software, die das abermalige Hochladen bereits vorhandener verleumde-

* Prof. Dr. *Johannes Hager* ist Universitätsprofessor an der Universität München (seit Ende März 2017 ist er pensioniert).

1 Die Zahl stammt aus dem Jahresbericht von Facebook von 2016.

2 Vgl den Sachverhalt bei LG Würzburg 11 O 2338/16 UVR BeckRS 2017, 103822.

3 Die Zahl stammt aus dem Jahresbericht von Facebook von 2016.

Fundstelle: *Hager*, Datenschutz in den sozialen Medien aus privatrechtlicher Perspektive, ALJ 2/2017, 95–104 (http://alj.uni-graz.at/index.php/alj/ article/view/90).

rischer Bilder automatisch blockiere. Das LG Würzburg hat den Erlass einer einstweiligen Verfügung abgelehnt, da nicht sicher beurteilt werden könne, ob die beantragte Sperre technisch machbar sei.[4]

II. Das Verhältnis von Datenschutz und Persönlichkeitsschutz

A. Damit stellt sich die Frage nach dem Verhältnis von Datenschutz und Persönlichkeitsrecht. Der Begriff des Datums wird weit gefasst; er enthält alle Informationen, die über eine Person etwas aussagen oder mit ihr in Verbindung zu bringen sind, auch Meinungsäußerungen und Tatsachenmitteilungen.[5] Insofern besteht im Schutzumfang kein Unterschied. Die frühere Rsp und hM gingen von einem Vorrang des Bundesdatenschutzgesetzes vor dem allgemeinen Persönlichkeitsrecht aus.[6] Begründet wurde das mit der vermeintlichen Subsidiarität des Persönlichkeitsrechts; angesichts der Regelung des dBDSG[7] liege dann keine Lücke vor.[8]

Nur gelegentlich hat man weitergehende Rechtsbehelfe, etwa einen Widerruf, für möglich erachtet.[9] Das war schon damals wenig überzeugend. Weil und soweit sich das Persönlichkeitsrecht auf grundrechtliche Garantien stützen kann, ist es nicht möglich, die kodifizierte Gewährleistung im dBDSG für abschließend zu halten. Das zeigt auch exemplarisch ein Fall, den der BGH zu entscheiden hat. Der Kläger hatte nach § 807 dZPO aF (= § 802 f dZPO nF) die eidesstattliche Versicherung abgegeben. Darüber hatte die beklagte Auskunftei berichtet. Der BGH hielt das nach § 32 dBDSGaF (= § 29 Abs 1 Z 1 dBDSG nF[10]) für zulässig.[11] Gesetzt den Fall, das hätte den grundgesetzlichen Vorgaben widersprochen, so hätte der Subsidiaritätsgedanke nicht einschlägig sein können, weil er Art 1 Abs 3 dGG und der Hierarchie der Normen widersprochen hätte. Vieles im dBDSG wirkt auch eher zufällig. Mag das Datenschutzrecht seinerseits auch bahnbrechend gewesen sein, so erscheint die Regelung der Übermittlung nach § 29 Abs 2 dBDSG heute doch etwas holzschnittartig, liest man nicht die im Rahmen des Persönlichkeitsrechts entwickelten Abwägungskriterien mit hinein. So bedarf es entgegen dem Wortlaut gerade nicht der glaubhaften einzelfallbezogenen Darlegung des berechtigten Interesses am Abruf der Dateien.[12] Die Normen des dBDSG sind daher auch angesichts des Schutzes der Meinungsfreiheit verfassungskonform auszulegen.[13]

---

4 LG Würzburg 11 O 2338/16 UVR BeckRS 2017, 103822.

5 BGH VI ZR 196/08 BGHZ 181, 328 (333) Rz 17; *Dammann* in *Simitis* (Hrsg), Bundesdatenschutzgesetz[8] (2014) § 3 Rz 77 ff; *Taeger* in *Taeger/Gabel* (Hrsg), Kommentar zum BDSG[2] (2013) § 29 Rz 26.

6 BGH VI ZR 273/79 BGHZ 80, 311 (319) = NJW 1981, 1738 (1740); VI ZR 105/82 BGHZ 91, 233 (238); VI ZR 244/84 NJW 1986, 2505 (2507); OLG Düsseldorf I 10 U 69/06 MMR 2007, 387; *Kamlah* in *Plath* (Hrsg), Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen vom TMG und TKG[2] (2016) § 35 BDSG Rz 57; *Gola* in *Gola/Schomerus/Klug/Körffer* (Hrsg), BDSG[12] (2015) § 35 Rz 25; *Meents/Hinzpeter* in *Taeger/Gabel*, BDSG[2] § 35 Rz 6; *Däubler* in *Däubler/Klebe/Wedde/Weichert* (Hrsg), Bundesdatenschutzgesetz[5] (2016) § 32 Rz 41; *Dix* in *Simitis*, Bundesdatenschutzgesetz[8] § 35 Rz 71; wohl auch *Stollhoff* in *Auernhammer* (Hrsg), Bundesdatenschutzgesetz[4] (2014) § 35 Rz 11; offen gelassen in BGH VI ZR 105/82 NJW 1984, 1886 f.

7 Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. 1. 2013 (dBGBl I 2013, 66), zuletzt geändert durch Art 1 des Gesetzes vom 28. 4. 2017 (dBGBl I 2017, 968).

8 BGH VI ZR 273/79 BGHZ 80, 311 (319) = NJW 1981, 1738 (1740); VI ZR 105/82 BGHZ 91, 233 (238); III ZR 159/82 NJW 1984, 436; *Kamlah* in *Plath*, BDSG[2] § 35 BDSG Rz 57.

9 *Brink* in *Wolff/Brink* (Hrsg), BeckOK Datenschutzrecht § 35 Rz 6 f (Stand 1. 2. 2017).

10 Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. 1. 2013 (dBGBl I 2013, 66), zuletzt geändert durch Art. 1 des Gesetzes vom 28. 4. 2017 (dBGBl I 2017, 968).

11 BGH VI ZR 244/84 NJW 1986, 2505 (2506).

12 BGH VI ZR 358/13 BGHZ 202, 242 (258) Rz 45.

13 BGH VI ZR 196/08 BGHZ 181, 328 (343 f) Rz 41.

B. Stillschweigend hat sich auch die Rsp vom Subsidiaritätsdogma verabschiedet.

1. In der Entscheidung www.spickmich.de stellt zwar der BGH den Löschungsanspruch nach § 35 dBDSG in den Mittelpunkt.[14] Letztendlich mündet die Überprüfung in der aus dem klassischen Persönlichkeitsrecht bekannten Abwägung zwischen Art 1, 2 dGG auf der einen und Art 5 dGG auf der anderen Seite.[15] Dabei geht es um die betroffene Sphäre,[16] um die Abgrenzung zwischen der Meinungsäußerung und der Tatsachenbehauptung[17] und schließlich um das Vorliegen einer Formalbeleidigung oder Schmähkritik,[18] also um Kategorien die beim allgemeinen Persönlichkeitsrecht die zentrale Rolle spielen. Auch in der Entscheidung „Ärzte-Portal II" beginnt die Prüfung mit § 35 dBDSG[19] und § 29 dBDSG,[20] wendet sich dann aber sehr schnell der Untersuchung anhand des allgemeinen Persönlichkeitsrechts zu.[21] Demgemäß ist § 29 Abs 2 Satz 1 dBDSG verfassungskonform dahin gehend auszulegen, dass die Zulässigkeit der Übermittlung der Daten an den abfragenden Nutzer aufgrund einer Gesamtabwägung zwischen dem Persönlichkeitsrecht des Betroffenen und dem Informationsinteresse des anderen Teils beurteilt werden muss.[22] Dabei soll es sogar einer einzelfallbezogenen Darlegung des berechtigten Interesses nicht bedürfen.[23] In der Entscheidung „Ärzte-Portal III" beschränkt sich der BGH nunmehr aber auf die Prüfung, ob das Persönlichkeitsrecht des kritisierten Arztes verletzt sei,[24] ohne das dBDSG noch zu erwähnen.

2. Auch das BAG (Bundesarbeitsgericht) räumt der grundrechtlichen Prüfung den Vorrang ein. Ob die §§ 6b, 32 dBDSG die Verwertung einer heimlichen Videoaufzeichnung zur Stützung der Kündigung eines Arbeitsverhältnisses erlaubten, könne offenbleiben. Denn jedenfalls ergebe sich das Verwertungsverbot aus dem allgemeinen Persönlichkeitsrecht des Arbeitnehmers, soweit nicht überwiegende Beweisinteressen des Arbeitgebers eingriffen.[25] Sei die Verwertung dagegen zulässig, stehe auch das Kennzeichnungsgebot des § 6b Abs 2 dBDSG nicht entgegen;[26] die Form sei verfassungskonform zu interpretieren.[27] Das umgekehrte Verständnis begegnete im Hinblick auf die durch Art 12 Abs 1 und Art 14 Abs 1 dGG gesicherten Interessen des Arbeitgebers verfassungsrechtlichen Bedenken.[28]

C. Damit stellt sich das Verhältnis zwischen dem dBDSG und dem Persönlichkeitsrecht nach den üblichen Regeln dar. Der Schutz des dBDSG ist nicht abschließend. Insbesondere kann auch jeweils des § 7 Abs 1 Satz 1 dBDSG und § 8 Abs 2 dBDSG eine Entschädigung wegen immaterieller Beeinträchtigung geschuldet sein, ohne dass es darauf ankommt, ob und inwieweit die Normen

14 BGH VI ZR 196/08 BGHZ 181, 328 (333) Rz 16 ff.
15 BGH VI ZR 196/08 BGHZ 181, 328 (338 ff) Rz 29 ff.
16 BGH VI ZR 196/08 BGHZ 181, 328 (338 f) Rz 30.
17 BGH VI ZR 196/08 BGHZ 181, 328 (339 f) Rz 33.
18 BGH VI ZR 196/08 BGHZ 181, 328 (340) Rz 34.
19 BGH VI ZR 358/13 BGHZ 202, 242 (245 f) Rz 11 ff.
20 BGH VI ZR 358/13 BGHZ 202, 242 (246 ff) Rz 14 ff.
21 BGH VI ZR 358/13 BGHZ 202, 242 (250 ff) Rz 25 ff.
22 BGH VI ZR 358/13 BGHZ 202, 242 (258) Rz 45.
23 BGH VI ZR 358/13 BGHZ 202, 242 (258) Rz 45.
24 BGH VI ZR 34/15 BGHZ 209, 139 (145) Rz 15 ff.
25 BAG 2 AZR 797/11 BAGE 146, 303 (315) Rz 42.
26 BAG 2 AZR 797/11 BAGE 146, 303 (319) Rz 51; BAG 2 AZR 848/15 NJW 2017, 843 (846) Rz 38.
27 BAG 2 AZR 153711 BAGE 142, 176, 187 Rz 41.
28 BAG 2 AZR 797/11 BAGE 146, 303 (319) Rz 51.

des dBDSG Schutzgesetze iSd § 823 Abs 2 dBGB sind.[29] Dies deutet dann auch die Rsp in einem Fall an, in dem ein Krankengutachten einer inzwischen verstorbenen Patientin persönlichkeitswidrig von der Krankenkasse in weiteren Verfahren verwendet worden war. Der Anspruch wurde abgelehnt, weil Forderungen wegen immaterieller Beeinträchtigungen nicht vererblich seien. Das überzeugt indes genauso wenig wie im vorangegangenen Fall des verstorbenen Entertainers Peter *Alexander*, der kurz nach Anhängigkeit, aber vor Rechtshängigkeit der Klage verstorben war und dessen Ansprüche angeblich mit seinem Tod erloschen waren.[30] Das dBDSG bringt also – durchaus wichtige – Aspekte, wird aber von den allgemeinen verfassungsrechtlich vorgeprägten oder gar determinierten Regeln des Persönlichkeitsrechts überformt oder jedenfalls ergänzt. Es kommt also zu einer Verschränkung der speziellen Regelungen des dBDSG und des Persönlichkeitsrechts – nicht anders als es etwa beim KUG und dem Persönlichkeitsrecht der Fall ist.[31]

III. Das Privileg der §§ 7 ff dTMG[32]

Die §§ 7 ff dTMG erscheinen auf den ersten Blick die Diensteanbieter zu privilegieren, soweit es nicht um eigene Informationen geht. Allerdings findet das Haftungsprivileg keine Anwendung auf Unterlassungsansprüche,[33] sondern betreffe nur die strafrechtliche Verantwortlichkeit und die Schadensersatzhaftung.[34]

A. Die Content-Provider sind jedenfalls verantwortlich. Das ist zumindest dann naheliegend, wenn es um selbst verfasste Informationen geht. Auch ist der Anwendungsbereich weiter, als es auf den ersten Blick erscheinen mag. Nicht jede zunächst von anderen in die Welt gesetzte Information bleibt eine fremde Information. Vielmehr spielt es eine entscheidende Rolle, wie die Nachrichten präsentiert werden.

1. Ein Paradebeispiel ist die Autocomplete-Funktion bei Suchmaschinen. Wenn man einen Begriff einzugeben beginnt, werden automatisch Ergänzungen vorgeschlagen. Die Betreiber der Suchmaschinen hatten sich mit dem Hinweis zu verteidigen versucht, die Funktion berichte nur darüber, dass vorherige Benutzer diese Kombination zur Recherche eingegeben hätten, oder

29 Vgl dazu den Überblick bei *J. Hager* in *Staudinger* (Hrsg), BGB (2009) § 823 Rz G 44; *Wagner* in *Säcker/Rixecker/Oetker/Limperg* (Hrsg), Münchener Kommentar zum Bürgerlichen Gesetzbuch[7] VI (2017) § 823 Rz 326; *Spickhoff* in *Soergel* (Hrsg), Kommentar zum BGB[13] XII (2005) § 823 Rz 239; *Gola* in *Gola/Schomerus/Klug/Körffer* (Hrsg), BDSG[12] (2015) § 1 Rz 3.

30 BGH VI ZR 246/12 BGHZ 201, 45 (48 ff) Rz 8 ff; *Teichmann* in *Jauernig* (Hrsg), BGB[16] (2015) § 253 Rz 13; *Stürner* in *Jauernig* (Hrsg), BGB[16] (2015) § 1922 Rz 12; *Staudinger* in *Schulze et al* (Hrsg) Bürgerliches Gesetzbuch[9] (2017) § 823 Rz 112; *Weidlich* in *Palandt* (Hrsg), BGB[76] (2017) § 1922 Rz 36; *Bamberger* in *Bamberger/Roth* (Hrsg), BeckOK-BGB (Stand 1. 2. 2017) § 823 Rz 118; *Leipold* in *Säcker/Rixecker/Oetker/Limperg* (Hrsg), Münchener Kommentar zum Bürgerlichen Gesetzbuch[7] X § 1922 Rz 120; *Slizyk* in *Slizyk* (Hrsg), IMM-DAT-Kommentar[13] (2017) Rz 465; *Staender-Vorwachs*, Vererblichkeit eines Geldentschädigungsanspruchs wegen Persönlichkeitsverletzung, NJW 2014, 2831 (2833); aA *J. Hager*, Allgemeines Persönlichkeitsrecht, JA 2014, 627 (629); *Kunz* in *Staudinger* (Hrsg), BGB (2016) § 1922 Rz 311 ff; BGH VI ZR 246/12 LMK 2014, 359158 unter 2 aE = ZUM 2014, 706 f (*Ludyga*) = JZ 2014, 1053 (1058 f) (*C. Schubert*); *Beuthien*, Zur Unvererblichkeit des Anspruchs auf Geldentschädigung für Persönlichkeitsrechtsverletzung, GRUR 2014, 957 (958); *Muscheler*, 10 Jahre Erbrecht – Rückblick und Ausblick, ErbR 2015, 650 (661).

31 *J. Hager* in *Staudinger* (Hrsg), BGB (2017) § 823 Rz C 149.

32 Telemediengesetz vom 26. 2. 2007 (BGBl I 2007, 179), zuletzt geändert durch Art 1 des Gesetzes vom 21. 7. 2016 (BGBl I 2007, 1766).

33 BGH I ZR 304/01 BGHZ 158, 236 (246); I ZR 35/04 BGHZ 172, 119 (126) Rz 19; VI ZR 93/10 BGHZ 191, 219 (225) Rz 19; VI ZR 34/15 BGHZ 209, 139 (146 f) Rz 19; VI ZR 101/06 NJW 2007, 2558 f Rz 7; VI ZR 144/11 NJW 2012, 2345 Rz 9; VI ZR 210/08 NJW-RR 2009, 1413 (1414) Rz 17; VI ZR 345/09 GRUR 2011, 552 (553) Rz 26; *J. Hager* in *Staudinger*, BGB (2017) § 823 Rz C 62b.

34 BGH I ZR 35/04 BGHZ 172, 119 (126) Rz 19; VI ZR 93/10 BGHZ 191, 219 (225) Rz 19; VI ZR 101/06 NJW 2007, 2558 (2559) Rz 7; *J. Hager* in *Staudinger*, BGB (2017) § 823 Rz C 62b.

dass sich diese Informationen in verlinkten Drittinhalten jeweils auffinden ließen.[35] Dem ist der BGH nicht gefolgt. Denn eine Suchmaschine leite nicht nur fremde Informationen durch oder speichere sie, sondern biete eigene Inhalte an; das sei eben das Ergebnis des Autocomplete-Hilfsprogramms.[36] Allerdings treffe den Betreiber erst dann eine Prüfpflicht, wenn er Kenntnis von der Verletzung habe.[37] Insofern ist das Problem mit demjenigen des Host-Providers identisch.[38] Eigene Inhalte liegen nicht nur dann vor, wenn sie selbst verfasst sind; es genügt auch, wenn der Betreffende sie sich zu eigen macht.[39]

2. Je nach Sachlage kann auch das Setzen eines Hyperlinks als Verletzungshandlung aufzufassen sein, wenn sich der Handelnde damit die Aussage zu eigen macht.[40] Hier kommt es dann entscheidend auf die Verletzung einer Verkehrspflicht an.[41]

3. Bei Snippets – also kurzen Inhaltsangaben – ist die Lage zwar heftig umstritten.[42] Doch kann letztendlich nichts anderes gelten als bei der Autocomplete-Funktion; auch hier generiert der Provider durch den Einsatz seiner Maschine erst den Inhalt der Mitteilung.

4. Einer besonderen Betrachtung bedürfen Internetarchive. Ein Beispiel ist der Bericht über den Mord an einem bekannten Münchner Schauspieler im Jahre 1990 und über die folgenden Prozesse gegen seine Mörder. Hier die Information löschen zu müssen würde die Archivfunktion des Internets – in der es durchaus vergleichbar mit Printmedien ist – gefährden.[43] Das entscheidende Kriterium ist, ob die Suche offen gehalten werden soll oder ob speziell auf die Information hingeführt wird.[44]

B. Sehr problematisch ist die Haftung des Host-Providers. Er vermittelt nur die Informationen anderer. Hierher kann in Sonderfällen auch die Denic gehören, soweit bereits in der Verwendung eines konkreten Namens eine Verletzung bestehen kann. Eine genaue Abgrenzung ist hier nicht nötig.[45] Diese Vermittler stellen zunächst ja nur den Speicherplatz bzw den Zugang zur Verfügung und scheinen nach § 10 dTMG privilegiert zu sein. Doch täuscht dieser erste Eindruck. Er täuscht

35 So auch die Beurteilung durch das OLG Köln 15 U 199/11 GRUR-RR 2012, 486 (489) als Vorinstanz zu BGH VI ZR 269/12 BGHZ 197, 213; Bericht bei BGH VI ZR 269/12 BGHZ 197, 213 (215 f) Rz 4.

36 BGH VI ZR 269/12 BGHZ 197, 213 (220) Rz 20; *J. Hager* in *Staudinger*, BGB (2017) § 823 Rz C 62c; *Söder* in *Bamberger/Roth* (Hrsg), BeckOK-BGB § 823 Rz 27 (Stand 1. 2. 2017); aA Vorinstanz OLG Köln I-15 U 199/11 ZUM 2012, 987 (991).

37 BGH VI ZR 269/12 BGHZ 197, 213 (224) Rz 30.

38 Vgl unten III.B.2. und 3.

39 BGH I ZR 166/07 NJW-RR 2010, 1276 (1278) Rz 22 f.

40 BGH I ZR 74/14 BGHZ 206, 103 (105 f) Rz 13; I ZR 102/05 NJW 2008, 1882 (1883 f) Rz 20; I ZR 166/07 NJW-RR 2010, 1276 (1278) Rz 22; OGH 4 Ob 274/00y MMR 2001, 518 (520).

41 *J. Hager* in *Staudinger*, BGB (2017) § 823 Rz C 62g.

42 Für Haftung KG 9 W 196/09 ZUM-RD 2010, 224 (225); LG Mönchengladbach 10 O 170/12 ZUM-RD 2014, 46 (48); LG Hamburg 324 O 660/12 NJW 2015, 796 (800); *J. Hager*, Das Persönlichkeitsrecht im europäischen, österreichischem und deutschem Recht, JBl 2013, 273 (282 f); eine Haftung ablehnend OLG Stuttgart 4 U 109/08 MMR 2009, 190; OLG Hamburg 7 U 70/09 MMR 2010, 490 (491); OLG München 29 U 1747/11 ZUM-RD 2012, 344 (346); KG 10 U 59/11 MMR 2012, 129.

43 BGH IV ZR 227/08 BGHZ 183, 353 (361 f) Rz 20; BGH VI ZR 243/08 NJW 2010, 2432 (2435) Rz 23; VI ZR 245/08 NJW 2010, 2728 (2730) Rz 21, 31; VI ZR 345/09 NJW 2011, 2285 (2288) Rz 21; VI ZR 217/08 NJW 2012, 2197 (2200) Rz 40; VI ZR 4/12 NJW 2013, 229 (230) Rz 15; VI ZR 330/11 GRUR 2013, 200 (201) Rz 17; *J. Hager* in *Staudinger*, BGB (2017) § 823 Rz C 226a.

44 EuGH 13. 5. 2014, C-131/12, *Google Spain* Rz 98 f; BGH IV ZR 227/08 BGHZ 183, 353 (361 f) Rz 20; VI ZR 245/08 NJW 2010, 2728 (2730) Rz 21, 31; VI ZR 345/09 NJW 2011, 2285 (2288) Rz 21; VI ZR 217/08 NJW 2012, 2197 (2200) Rz 44; VI ZR 330/11 GRUR 2013, 200 (201) Rz 18; *J. Hager* in *Staudinger*, BGB (2017) § 823 Rz C 226a.

45 *Seitz* in *Hoeren/Sieber/Holznagel* (Hrsg), Multimedia-Recht (2016) VIII Rz 12.

schon deshalb, weil die Norm nicht die Störerhaftung regelt,[46] sondern nur die strafrechtliche Verantwortung und die Schadensersatzpflicht des Diensteanbieters.[47]

1. Allerdings war die deutsche Rsp am Anfang sehr zurückhaltend was den Begriff des Störers angeht. Bei einer markenrechtlichen Entscheidung betont der BGH, dass es der Beklagten – in diesem Fall der Denic – nur dann zumutbar sei, die Registrierung eines Domain-Namens abzulehnen oder sie aufzuheben, wenn unschwer zu erkennen sei, dass die Nutzung dieses Namens Rechte Dritter beeinträchtige.[48] Generell sei die sinnvolle Nutzung der unübersehbaren Informationsfülle des Internets ohne Suchdienste praktisch ausgeschlossen.[49] Auch hier haben sich die Maßstäbe geändert. Der Host-Provider ist verantwortlich, sobald er Kenntnis von der Rechtsverletzung hat.[50] Eine derartige Kenntnis folgt regelmäßig aus der Beanstandung eines Betroffenen.[51] Der Betreiber eines Internetforums ist Herr des Angebots; der Betroffene kann Löschungs- und Unterlassungsansprüche auch gegen ihn richten.[52]

2. Der Störerbegriff wird dabei von den verschiedenen Senaten des BGH recht uneinheitlich definiert, ohne dass es in der Sache zu großen Differenzen kommt. Der I. Senat behandelt denjenigen als Störer, der – ohne Täter oder Teilnehmer zu sein – in irgendeiner Weise willentlich und adäquat kausal zur Verletzung des geschützten Rechtsguts beiträgt.[53] Der VI. Senat bezeichnet als Störer, wer die Störung willentlich und adäquat kausal verursacht.[54] Dabei genügt auch die Unterstützung oder die Ausnutzung der Handlung eines eigenverantwortlichen Dritten, sofern der in Anspruch Genommene die rechtliche Möglichkeit zur Verhinderung dieser Handlung hatte.[55] Der V. Senat fordert, dass die Störung zumindest mittelbar auf den Eigentümer oder Besitzer der störenden Sache zurückgeht.[56] Sieht man näher zu, so geht es nicht um den Begriff des Störers; in Rede steht vielmehr die Täterschaft. Wer weiß, dass er stört, handelt mit Vorsatz und ist deswegen nicht nur zum Unterlassen, sondern ab dem Zeitpunkt der Kenntnis auch zum Schadensersatz verpflichtet.

3. Damit sind die Pflichten des Host-Providers nicht abschließend beschrieben. Den Betreiber können zusätzliche Prüfpflichten treffen.[57] Diese Prüfpflichten sind unterschiedlich zu beschreiben; sie hängen ab vom Gewicht der angezeigten Rechtsverletzung sowie von den Erkenntnis

46 BGH I ZR 304/01 BGHZ 158, 236 (248); VI ZR 196/08 BGHZ 181, 328 (332) Rz 14; VI ZR 101/06 NJW 2007, 2558.
47 BGH VI ZR 196/08 BGHZ 181, 328 (332) Rz 14; VI ZR 101/06 NJW 2007, 2558 (2559).
48 BGH I ZR 251/99 BGHZ 148, 13 (18); I ZR 120/96 GRUR 1999, 418 (419); OGH 4 Ob 166/00 GRUR-Int 2001, 790 (792); 4 Ob 194/05s GRUR-Int 2006, 955 (956): *„Auch für einen juristischen Laien ohne weitere Nachforschungen offenkundig"*.
49 BGH I ZR 259/00 BGHZ 156, 1 (18 f).
50 BGH I ZR 304/01 BGHZ 158, 236 (251 f); I ZR 18/04 BGHZ 173, 188 (203) Rz 47; I ZR 57/09 BGHZ 191, 19 (26) Rz 21; VI ZR 93/10 BGHZ 191, 219 (226) Rz 24; VI ZR 34/15 BGHZ 209, 139 (148) Rz 23.
51 BGH VI ZR 93/10 BGHZ 191, 219 (227 f) Rz 22; VI ZR 34/15 BGHZ 209, 139 (148) Rz 23.
52 BGH VI ZR 196/08 BGHZ 181, 328 (332) Rz 14.
53 BGH I ZR 304/01 BGHZ 158, 236 (251) (unter Berufung auf BGH I ZR 251/99 BGHZ 148, 13 (17)); I ZR 121/08 BGHZ 185, 330 (335) Rz 19; I ZR 57/09 BGHZ 191, 19 (24) Rz 20; I ZR 174/14 BGHZ 208, 82 (91) Rz 21; I ZR 80/12 NJW 2013, 3245 (3247) Rz 30; I ZR 22/99 NJW-RR 2002, 832 (833).
54 BGH VI ZR 93/10 BGHZ 191, 219 (225) Rz 21 f; VI ZR 269/12 BGHZ 197, 213 (222) Rz 24; VI ZR 340/14 BGHZ 206, 289 (301) Rz 34; VI ZR 34/15 BGHZ 209, 139 (147) Rz 22; VI ZR 373/02 NJW 2004, 762 (765).
55 BGH VI ZR 269/12 BGHZ 197, 213 (222) Rz 24; VI ZR 340/14 BGHZ 206, 289 (301) Rz 34.
56 BGH V ZR 44/10 NJW 2011, 753 (754) Rz 13.
57 BGH I ZR 317/01 BGHZ 158, 343 (352 ff); I ZR 121/08 BGHZ 185, 330 (336) Rz 19; VI ZR 93/10 BGHZ 191, 219 (226) Rz 21; I ZR 18/11 BGHZ 194, 339 (345) Rz 19; I ZR 174/14 BGHZ 208, 82 (91) Rz 21; VI ZR 34/15 BGHZ 209, 139 (153) Rz 38; I ZR 124/03 NJW 2006, 2764 (2766) Rz 32; I ZR 80/12 NJW 2013, 3245 (3247) Rz 70; I ZR 73/05 NJW-RR 2008, 1138 (1139) Rz 50; I ZR 155/09 GRUR 2011, 617 (619) Rz 37.

möglichkeiten des Providers.[58] Zu berücksichtigen sind die Zumutbarkeit,[59] Funktion und Aufgabenstellung des vom Provider betriebenen Dienstes und die Eigenverantwortung des Nutzers.[60] Damit wird allerdings auf Verschulden abgestellt und nicht auf die bloße Störung. Es geht dann um die Verkehrspflicht zum Schutz der fremden Persönlichkeit,[61] wie sie etwa aus der Recherchepflicht der Presse bekannt ist.[62] Der Portalbetreiber muss ernsthaft versuchen, sich die notwendige Tatsachengrundlage zu verschaffen.[63]

4. Ein besonderes Problem stellt die Nennung des Täters dar. In Österreich treten allerdings wegen § 18 Abs 4 ECG in dieser Hinsicht keine Fragen auf. Der Betroffene hat unter den dort genannten Voraussetzungen ein Recht auf Auskunft.

a. Der BGH hat dagegen für das deutsche Recht wegen § 12 Abs 2 dTMG ein Recht des Verletzten verneint, den Namen des Täters genannt zu bekommen. Eine Verwendung von Daten liege auch bei einer Übermittlung an Dritte vor.[64] Die Herbeiführung des geschuldeten Erfolgs – die Auskunft – sei angesichts von § 12 Abs 2 dTMG unmöglich. Es fehle an einer Rechtsvorschrift, die dies erlaube, ebenso natürlich an der Einwilligung des Autors.[65] § 242 dBGB enthalte keine Erlaubnis iSd § 12 Abs 2 dTMG.[66] Auch § 14 Abs 2 dTMG greife nicht ein, da die dort genannten Zwecke nicht einschlägig seien.[67] Auch eine Analogie zu den § 14 Abs 2, § 15 Abs 5 Satz 4 dTMG scheide mangels einer Lücke aus.[68] Man mag so entscheiden, wenn die Inhalte rechtmäßig sind und deshalb ohnehin keine Ansprüche gegen den Autor in Frage kommen.[69]

b. Anders liegt es dagegen, wenn eine Rechtsverletzung gegeben ist.[70] Denn der Schutz der Persönlichkeit ist verfassungsrechtlich gefordert.[71] Daran kann das dTMG als Norm des einfachen Rechts nichts ändern. So ist schon unklar, warum die Möglichkeit, vom Host-Provider Abhilfe verlangen zu können,[72] den Anspruch gegen den Täter ausschließen soll. Auch ist nicht einzusehen, warum die anonyme Nutzung im Internet stets zulässig[73] oder ihm gar immanent sein soll.[74] Die Lage ist vielmehr geradewegs umgekehrt. Neben dem Autor können weitere Personen als Störer zur Unterlassung verpflichtet sein, so der Verleger,[75] die Sendeanstalt,[76] der Redakteur[77]

58 BGH VI ZR 93/10 BGHZ 191, 219 (226 f) Rz 22 und Rz 26; VI ZR 34/15 BGHZ 209, 139 (153) Rz 38.
59 BGH I ZR 251/99 BGHZ 148, 13 (17); I ZR 304/01 BGHZ 158, 236 (251); I ZR 317/01 BGHZ 158, 343 (350); I ZR 57/09 BGHZ 191, 19 (25) Rz 20; VI ZR 93/10 BGHZ 191, 219 (226) Rz 22; VI ZR 210/08 NJW-RR 2009, 1413 (1414) Rz 18.
60 BGH I ZR 304/01 BGHZ 158, 236 (251 f); VI ZR 93/10 BGHZ 191, 219 (226) Rz 22; I ZR 169/12 BGHZ 200, 76 (82) Rz 22; VI ZR 34/15 BGHZ 209, 139 (153) Rz 38; VI ZR 210/08 NJW-RR 2009, 1413 (1415) Rz 18; I ZR 240/12 GRUR 2015, 485 (490) Rz 50.
61 *J. Hager* in *Staudinger*, BGB (2017) § 823 Rz C 110.
62 *J. Hager* in *Staudinger*, BGB (2017) § 823 Rz C 112.
63 BGH VI ZR 34/15 BGHZ 209, 139 (155) Rz 42.
64 BGH VI ZR 345/13 BGHZ 201, 380 (383 f) Rz 9 ff; VI ZR 358/13 BGHZ 202, 242 (254 f) Rz 36 f; *Giebel*, Zivilrechtlicher Rechtsschutz gegen Cybermobbing in sozialen Netzwerken, NJW 2017, 977; anders noch BGH VI ZR 105/82 BGHZ 91, 233 (241); aA *Seitz* in *Hoeren/Sieber/Holznagel* (Hrsg), Multimedia-Recht (2012) VIII Rz 72.
65 BGH VI ZR 345/13 BGHZ 201, 380 (383 f) Rz 10.
66 BGH VI ZR 345/13 BGHZ 201, 380 (384) Rz 11.
67 BGH VI ZR 345/13 BGHZ 201, 380 (384 f) Rz 12.
68 BGH VI ZR 345/13 BGHZ 201, 380 (385) Rz 13 ff.
69 So lag es nach Meinung des BGH VI ZR 196/08 BGHZ 181, 328 (338 ff) Rz 30 ff.
70 Sie kam im Fall BGH VI ZR 34/15 BGHZ 209, 139 (250 ff) Rz 29 ff in Betracht.
71 BGH VI ZR 34/15 BGHZ 209, 139 (150 ff) Rz 29 ff.
72 So BGH VI ZR 196/08 BGHZ 181, 328 (341) Rz 38; VI ZR 358/13 BGHZ 202, 242 (254) Rz 36.
73 BGH VI ZR 34/15 BGHZ 209, 139 (153) Rz 38.
74 So aber BGH VI ZR 358/13 BGHZ 202, 242 (256) Rz 41.
75 BGH I ZR 8/51 BGHZ 3, 270 (275 f); I ZR 38/53 BGHZ 14, 163 (174); VI ZR 101/06 NJW 2007, 2558 (2559) Rz 13.
76 BGH VI ZR 246/74 BGHZ 66, 182 (188); VI ZR 101/06 NJW 2007, 2558 (2559) Rz 13.
77 BGH VI ZR 55/62 BGHZ 39, 124 (129 f); VI ZR 16/73 NJW 1974, 1762; VI ZR 68/73 VersR 1974, 1080.

oder eben der Betreiber einer Internetplattform.[78] Die Tatsache, dass die Identität des Täters dem Verletzten bekannt ist, lässt die Haftung des Forenbetreibers nicht entfallen,[79] erst recht aber nicht diejenige des Täters. § 13 Abs 6 dTMG, dessen Eingreifen der BGH offen gelassen hat,[80] steht nicht entgegen; die Norm ist unter verfassungsrechtlichen Aspekten zum Schutz der Persönlichkeit zu korrigieren. Das ist übrigens kein Sonderfall. Auch eine Versteigerung im Internet lässt sich kaum sinnvoll durchführen, wenn der Bieter anonym oder pseudo-anonym verbleibt.[81] Es überzeugt daher auch nicht undifferenziert, dass es mit Art 5 Abs 1 Satz 1 dGG nicht vereinbar sein soll, dass die geäußerte Meinung ihrem Verfasser zugeordnet werden könne.[82] Zwar kann sich die Presse im Rahmen des Art 5 Abs 1 Satz 2 dGG auf die Verletzung der Meinungsfreiheit anderer berufen[83] und es in diesem Zusammenhang gestattet sein, Zuschriften auch anonym abzudrucken.[84] Doch kann das wiederum nur gelten, wenn die Inhalte als solche rechtmäßig sind. Rechtswidrige Äußerungen stehen nicht unter dem Schutz des Art 5 dGG und können daher nicht an seiner Garantie teilhaben. Eine entsprechende Ausnahme sieht etwa auch § 97 Abs 2 Satz 3, Abs 5 Satz 2 dStPO vor. Man könnte – dürften die Autoren rechtswidriger Inhalte geheim bleiben – nur die Verbreiter in Anspruch nehmen; diese Vorstellung wäre etwa bei einer Zeitung oder auch einer Rundfunksendung kaum überzeugend. Wird der Autor nicht genannt und braucht er auch vom Host-Provider nicht offenbart zu werden, bleibt der Persönlichkeitsschutz an einer empfindlichen Stelle lückenhaft. So könnten etwa bereits entstandene Schäden – seien sie materieller Art, seien sie immaterieller Art – nicht liquidiert werden. Wenn die Entschädigung unmittelbar aus dem dGG folgt,[85] so darf diese Rechtsfolge nicht dadurch unterlaufen werden, dass der Betroffene keine Möglichkeit hat, den Täter ausfindig zu machen.

c. Der BGH erlegt dem Host-Provider eine besondere Überprüfungspflicht auf. Er müsse dem Bewertenden die Beanstandung des betroffenen Arztes übersenden und ihn zur Stellungnahme auffordern. So sei er etwa gehalten, um die – insbesondere zeitliche – Präzisierung des Behandlungskontakts zu bitten – wiederum mit der Möglichkeit des Bewertenden, zur Vermeidung seiner Identifizierung ein größeres Zeitfenster zu nennen.[86] Reagiere er nicht, so sei das Vorbringen des betroffenen Arztes als zutreffend zu unterstellen und die Löschung vorzunehmen; sei die Auskunft ausreichend und präzisiere der betroffene Arzt dann seinerseits nicht weiter, so habe die Löschung zu unterbleiben.[87] Das ist in mehrfacher Hinsicht wenig überzeugend. Der Host-Provider wird in eine Rolle gedrängt, wie sie nur dem Richter zusteht. So kann es um komplexe Rechtsfragen gehen. Auch können Umstände des Einzelfalls – etwa das Recht zum Gegenschlag – vorliegen, die erst die Entscheidung ermöglichen. Diese Klärung ist Aufgabe der Judikative und nicht des Host-Providers.

78 BGH VI ZR 101/06 NJW 2007, 2558 (2559) Rz 13.
79 BGH VI ZR 101/06 NJW 2007, 2558 (2559) Rz 13.
80 BGH VI ZR 345/13 BGHZ 201, 380 (383) Rz 8.
81 *Jandt/Schaar/Schulz* in *Roßnagel* (Hrsg), Beck'scher Kommentar zum Recht der Telemediendienste (2013) § 13 TMG Rz 122.
82 BGH VI ZR 196/08 BGHZ 181, 328 (341) Rz 38; VI ZR 358/13 BGHZ 202, 242 (256) Rz 41; aM OLG Frankfurt 16 U 125/11 NJW 2012, 2896 (2897); *Grabenwarter* in *Maunz/Dürig* (Hrsg), Grundgesetz-Kommentar (2013) Art 5 Rz 86.
83 *Grabenwarter* in *Maunz/Dürig*, GG Art 5 Rz 89.
84 BVerfG 1 BvR 1183/90 BVerfGE 95, 28 (36).
85 BGH VI ZR 56/94 BGHZ 128, 1 (15).
86 BGH VI ZR 34/15 BGHZ 209, 139 (153 ff) Rz 37 ff und Rz 43.
87 BGH VI ZR 93/10 BGHZ 191, 219 (227 f) Rz 26 f.

C. Schließlich ist entgegen Zweifeln, die namentlich der OGH gehabt hatte und die ihn zur Vorlage an den EuGH veranlasst hatten,[88] auch der Access-Provider grundsätzlich verpflichtet, gegen die Störungen einzuschreiten, den Zugang zu sperren[89] oder zumindest durch ein Passwort zu sichern.[90] Auch hier ist an Prüfpflichten zu denken.[91] Die weitere Einschränkung, das Verbot gegen den Access-Provider sei nicht zumutbar, wenn der Betroffene nicht vorrangig gegen den Host-Provider vorgegangen sei,[92] vermag nicht zu überzeugen. Ein Rangverhältnis gibt es bei verschiedenen Störern nicht.[93]

IV. Besonderheiten des Gerichtsstands

A. Die örtliche und damit auch die internationale Zuständigkeit ergibt sich aus Art 7 Z 2 EuGVVO bzw – soweit es um die Schweiz, Island und Norwegen geht – aus Art 5 LugÜ II. Ansonsten sind die deutschen Gerichte nach § 32 dZPO zuständig. Hier hat der EuGH eine zumindest partiell restriktive Interpretation entwickelt, was die europäischen Normen angeht. Der Kläger kann die Verletzung von Persönlichkeitsrechten, die durch Inhalte auf einer Website hervorgerufen wird, entweder bei dem Gericht des Mitgliedstaates geltend machen, in dem der Urheber dieser Inhalte seine Niederlassung hat,[94] oder bei den Gerichten des Mitgliedstaates, in dem sich der Mittelpunkt der Interessen des Betroffenen befindet;[95] dort kann er den gesamten entstandenen Schaden liquidieren. Konsequenterweise darf der Schaden nicht ausschließlich im Hoheitsgebiet eines anderen Staates entstanden sein.[96] Er kann aber auch in jedem anderen Mitgliedstaat gegen den Verletzer vorgehen; doch sind diese nur zur Entscheidung über denjenigen Schaden zuständig, der im Hoheitsgebiet des Mitgliedstaates entstanden war.[97] Diese Regeln werden auch auf Unterlassungsansprüche erstreckt.[98]

B. Das ist wenig überzeugend. Schon die Entstehung der Rsp ist merkwürdig. Die Differenzierung wird nicht näher begründet. Sie widerspricht auch dem allgemeinen Grundsatz, dass jeder Erfolgsort den deliktischen Gerichtsstand hinsichtlich des gesamten Schadens begründet.[99] Man kommt auch zu dem seltsamen Ergebnis, dass das in Frankreich lebende Opfer in Deutschland

88 OGH 4 Ob 6/12d BeckRS 2012, 15042 = ZUM-RR 2012, 645 ff.

89 EuGH 27. 3. 2014, C-314/12, *UPC Telekabel Wien GmbH/Constantin Film Verleih GmbH ua* Rz 42 ff; I ZR 174/14 BGHZ 208, 82 (101 ff) Rz 45 ff.

90 EuGH 15. 9. 2016, C-484/14, *Mc Fadden/Sony Music* Rz 96.

91 BGH I ZR 174/14 BGHZ 208, 82 (96 f) Rz 32.

92 BGH I ZR 174/14 BGHZ 208, 82 (115 ff) Rz 82 ff.

93 BGH VI ZR 23/72 NJW 1976, 799 (800); VI ZR 169/85 NJW 1986, 2503 (2504); I ZR 56/55 GRUR 1957, 352 (353); *Herrler* in *Palandt* (Hrsg), BGB[76] (2017) § 1004 Rz 26; *J. Hager* in *Staudinger*, BGB (2017) § 823 Rz C 62j.

94 EuGH 25. 10. 2011, C-509/09, *eDate AdvertisingGmbH/X und martinez/MGN Limited* Rz 42 und Rz 52; BGH I ZR 35/11 NJW 2015, 1690 (1691) Rz 19; I ZR 91/11 NJW 2016, 2335 (2336) Rz 17; VI ZR 678/15 NJW 2017, 827 (829) Rz 18.

95 EuGH 25. 10. 2011, C-509/09, *eDate Advertising* Rz 48 und 52; 28. 1. 2015, C-375/13*, Kolassa/Barclays Bank plc* Rz 50 ff; BGH I ZR 35/11 NJW 2015, 1690 (1691) Rz 19; I ZR 91/11 NJW 2016, 2335 (2336) Rz 17; VI ZR 678/15 NJW 2017, 827 (829) Rz 18.

96 EuGH 10. 6. 2004, C-168/02, *Kronhofer/Maier ua* Rz 21; 28. 1. 2015, C-375/13*, Kolassa/Barclays Bank plc* Rz 49.

97 EuGH 7. 3. 1995, C-68/93, *Shevill ua/Presse Alliance SA* Rz 33; 25. 10. 2011, C-509/09, *eDate Advertising* Rz 51 f; 3. 10. 2013, C-179/12, *Pinckney/KDG Mediatech AG* Rz 47; BGH VI ZR 678/15 NJW 2017, 827 (829) Rz 19; *Hüßtege* in *Thomas/Putzo*, ZPO[38] (2017) Art 7 EuGVVO Rz 30; skeptisch *Stadler* in Musielak/Voit (Hrsg), ZPO[14] (2017) Art 7 EuGVVO Rz 20.

98 EuGH 25. 10. 2011, C-509/09, *eDate Advertising* Rz 35; 1. 10. 2002, C-167/00, *Verein für Konsumenteninformation/Henkel* Rz 48; BGH VI ZR 217/08 NJW 2012, 2197 (2198) Rz 17; I ZR 131/12 NJW 2014, 2504 (2505) Rz 16; VI ZR 678/15 NJW 2017, 827 (829) Rz 19; *Hüßtege* in *Thomas/Putzo*, ZPO[38] Art 7 EuGVVO Rz 30.

99 BGH IX ZR 32/93 BGHZ 124, 237 (245); XII ZR 181/93 BGHZ 132, 105 (111); VI ZR 23/09 BGHZ 184, 313 (316 f) Rz 8; IX ZR 176/10 BGHZ 189, 320 (330) Rz 21; VI ZR 111/10 NJW 2011, 2059 f Rz 7; *Patzina* in *Rauscher/Krüger* (Hrsg), Münchener Kommentar zur Zivilprozessordnung mit Gerichtsverfassungsgesetz und Nebengesetzen[5] (2016) § 32 Rz 20; *Roth* in *Stein/Jonas* (Hrsg), Zivilprozessordnung[23] (2014) § 32 Rz 26.

nur begrenzt den Schaden gegenüber dem in Italien agierenden Täter liquidieren kann. Das wäre anders, wenn der Täter in einem Land außerhalb des Geltungsbereichs der EuGVVO die Persönlichkeit des Opfers verletzt. Gemäß Art 6 Abs 1 EuGVVO ist dann deutsches Recht also § d32 ZPO anwendbar; damit kann in Deutschland der gesamte Schaden eingeklagt werden.[100] Das ist ein wenig plausibles Ergebnis. Das gilt auch – und erst recht – für Unterlassungsansprüche.

V. Zusammenfassung

1. Das dBDSG und das Persönlichkeitsrecht ergänzen sich. Namentlich ist das Persönlichkeitsrecht entgegen der früheren Rsp nicht subsidiär gegenüber dem Datenschutz.

2. Vom Privileg der §§ 7 ff dTMG werden die Provider nicht erfasst, soweit sie entweder die Informationen selbst gefertigt haben oder aber wissen, dass auf ihren Servern rechtswidrige Inhalte liegen bzw dass sie den Zugang zu Servern mit rechtswidrigen Inhalten ermöglichen. § 12 Abs 2 dTMG ist ebenso wie § 13 Abs 6 dTMG zum Schutz der Persönlichkeit entsprechend zu korrigieren; der Internetforenbetreiber ist daher verpflichtet, den Autor des störenden Beitrags zu benennen.

3. Entgegen der Rsp des EuGH sind sowohl Begehungs- als auch Erfolgsort gerichtsstandsbegründend – ohne Rücksicht darauf, in welchem Staat die Schäden entstanden sind.

100 Vgl zB BGH VI ZR 288/12 NJW-RR 2013, 1448 (1449) Rz 9 (Türkei).

AUSTRIAN LAW JOURNAL

ISSN: 2409-6911

DOI: 10.25364/1.4:2017.2.5
www.austrian-law-journal.at

Datenschutz in den sozialen Medien aus privatrechtlicher Perspektive

Stefan Perner*, Universität Linz

***Kurztext**: Der vorliegende Kommentar bezieht sich auf den Beitrag „Datenschutz in den sozialen Medien aus privatrechtlicher Perspektive" von Johannes Hager (ALJ 2/2017, 95) und beleuchtet einige österreichische Besonderheiten. Vor allem das Verhältnis des Datenschutzes in der digitalen Welt zum Schutz von Persönlichkeitsrechten ist nach wie vor sehr aktuell und wirft zahlreiche Probleme auf.*

***Schlagworte:** Auskunftsanspruch, Datenschutz, Persönlichkeitsrechte, soziale Medien.*

I. Einleitung

Rechtliche Aspekte des Datenschutzes in der digitalen Welt und sein Verhältnis zum Schutz von Persönlichkeitsrechten haben in den letzten Jahren nichts an Aktualität verloren. Gleiches gilt für Fragen der Verantwortlichkeit von Host-Providern und Plattformen für die dargebotenen Inhalte.

Die Fragen und juristischen Probleme, die sich in diesem Zusammenhang ergeben, beschränken sich naturgemäß nicht auf die nationale Ebene. Sie stellen sich vielmehr in Österreich genauso wie in Deutschland und darüber hinaus auf europäischer sowie weltweiter Ebene.

Dies zeigen schon die neuen europäischen Entwicklungen im Hinblick auf die Datenschutz-Grundverordnung (DSGVO)[1] und den Vorschlag für eine Richtlinie über das Urheberrecht im digitalen Binnenmarkt[2], der in Art 13 eine Regelung zur Verantwortlichkeit von Diensteanbietern der Informationsgesellschaft enthält, die große Mengen der von ihren Nutzern hochgeladenen Werke und sonstigen Schutzgegenstände speichern oder zugänglich machen.[3]

Bei all diesen Fragen fällt auf, dass man einerseits auf die Regelungen und Grundlagen im „analogen Bereich" zurückgreift, die Digitalisierung andererseits aber auch spezifische neue Fragen aufwirft.

---

* Univ.-Prof. Dr. *Stefan Perner* ist Universitätsprofessor am Institut für Zivilrecht der Johannes Kepler Universität Linz.

1 VO (EU) 679/2016 des Europäischen Parlaments und des Rates vom 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 2016/119, 1.

2 Vorschlag für eine Richtlinie über das Urheberrecht im digitalen Binnenmarkt vom 14. 9. 2016, COM(2016) 593 final.

3 Angesprochen sind damit große Plattformen wie YouTube.

Fundstelle: *Perner*, Datenschutz in den sozialen Medien aus privatrechtlicher Perspektive, ALJ 2/2017, 105–109 (http://alj.uni-graz.at/index.php/alj/ article/view/89).

II. Der Schutz von Persönlichkeitsrechten in der österreichischen Rechtsordnung

Der Schutz von Persönlichkeitsrechten und die Frage nach den Folgen einer Persönlichkeitsrechtsverletzung waren bislang schon in der analogen Welt ein breitgefächertes juristisches Thema, das in den letzten Jahrzehnten zunehmend an Bedeutung gewonnen hat. Der Schutz von Persönlichkeitsrechten im Internet wirft aus österreichischer Perspektive keine grundsätzlich neuen Fragen auf. Vielmehr kann hier sogar auf die Stammfassung des ABGB aus dem Jahr 1811 zurückgegriffen werden. Im – immer noch unveränderten – § 16 ABGB findet sich nämlich die von naturrechtlichen Vorstellungen geprägte Aussage, dass jeder Mensch angeborene, durch die Vernunft einleuchtende Rechte habe und daher als eine Person zu betrachten sei. Diese Norm, die zunächst als bloß programmatischer Grundsatz betrachtet wurde,[4] wird mittlerweile von der ständigen Rechtsprechung als *die* Zentralnorm der Rechtsordnung angesehen, die die Persönlichkeit als Grundwert anerkennt.[5] Aus ihr wird – so wie aus anderen durch die Rechtsordnung geschützten Grundwerten (zB Art 8 EMRK) – das jedermann angeborene Persönlichkeitsrecht auf Achtung seines Privatbereiches und seiner Geheimsphäre abgeleitet.[6]

Daneben bestehen aber noch zahlreiche Einzelvorschriften im ABGB und in anderen Gesetzen, die dem Schutz von Persönlichkeitsrechten dienen. Im Zusammenhang mit Persönlichkeitsverletzungen in sozialen Medien sind hierbei allen voran der Schutz der Privatsphäre in § 1328a ABGB, der Schutz der Ehre in § 1330 ABGB, der Bildnisschutz nach § 78 UrhG und der Persönlichkeitsschutz gegenüber Medien in §§ 6 ff MedienG zu nennen. Vor diesem Hintergrund liegt die Bedeutung des allgemein gehaltenen § 16 ABGB vor allem in seiner Auffangfunktion. Soweit das nicht bereits durch besondere einfachgesetzliche Normen geschieht, transportiert § 16 ABGB die verfassungsmäßig garantierten Grundrechte in das Privatrecht. Diese dienen nicht nur der Absicherung der fundamentalen Freiheiten und Rechte der Bürger gegenüber der Staatsmacht, sondern haben darüber hinaus auch Auswirkungen auf das Verhältnis der Bürger untereinander, indem die durch sie verkörperten Wertungen bei der Auslegung und Lückenfüllung privatrechtlicher Beziehungen zu berücksichtigen sind.[7]

Wegen des durch § 16 ABGB umfassend gewährleisteten Persönlichkeitsschutzes wird ein Unterlassungsanspruch gegen die Verletzung von Persönlichkeitsrechten auch in jenen Fällen angenommen, in denen ein solcher Anspruch nicht ausdrücklich vorgesehen ist.[8] Weitere mögliche Rechtsfolgen sind bspw ein Anspruch auf Schadenersatz und ein Beseitigungsanspruch.[9]

III. Das Verhältnis von Datenschutz und Persönlichkeitsschutz

Das Grundrecht auf Datenschutz ist in Österreich als Bestimmung im Verfassungsrang direkt im Datenschutzgesetz 2000 verankert (§ 1 DSG). Dort sind auch die konkreten Rechte des Betroffenen normiert – nämlich der Anspruch auf Geheimhaltung und die Begleitrechte auf Auskunft, Richtigstellung und Löschung bestimmter personenbezogener Daten.

4 Siehe nur *Posch* in *Schwimann/Kodek* (Hrsg), ABGB – Praxiskommentar[4] (2011) § 16 ABGB Rz 1 mwN.
5 *Schauer* in *Kletečka/Schauer* (Hrsg), ABGB-ON[1.02] § 16 Rz 5 mwN.
6 RIS-Justiz RS0008993; zB OGH 4 Ob 99/94 SZ 67/173.
7 OGH 8 Ob 108/05 y SZ 2005/185.
8 *Posch* in *Schwimann/Kodek*, ABGB[4] § 16 ABGB Rz 53 mwN.
9 *Schauer* in *Kletečka/Schauer*, ABGB-ON[1.02] § 16 Rz 28 ff.

Das Recht auf Datenschutz hat im Zusammenhang mit Persönlichkeitsrechtsverletzungen im Internet, insb in sozialen Medien, zwei Seiten. Auf der einen Seite bestehen weitreichende Überschneidungen mit den bereits erwähnten Bestimmungen zum Schutz der Persönlichkeit, weil das DSG ganz ähnliche Zielsetzungen und Wertungen hat.[10] Geschützt sind alle personenbezogenen Daten, also Informationen über eine bestimmte oder bestimmbare natürliche Person. So berührt zB die Verwendung von Bilddaten das besondere Persönlichkeitsrecht am eigenen Bild.

Andererseits steht das Datenschutzrecht aber im Zusammenhang mit Persönlichkeitsrechtsverletzungen im Internet oft aus der Perspektive des Rechtsverletzers im Fokus. Dies liegt daran, dass es für die verletzte Person schwierig bis unmöglich ist, die Identität des Rechtsverletzers herauszufinden. Wendet sich die in ihren Persönlichkeitsrechten verletzte Person an den für sie greifbaren Host-Provider, so wird dieser reflexartig das Recht auf Datenschutz des Rechtsverletzers einwenden wollen. Es geht hier also im Grunde um eine Kollision von Grundrechten und die Abwägungspflichten, die den Host-Provider in einer solchen Situation treffen können. Die Rolle des Vermittlers ist hier eine besonders heikle. Es verwundert nicht, dass die rechtliche Klarstellung der Verantwortlichkeit des Vermittlers in mehreren Zusammenhängen, so etwa auch bei Urheberrechtsverletzungen,[11] eine der drängendsten Fragen der digitalen Welt ist.

Anders als in Deutschland, wo der BGH[12] in diesem Zusammenhang entschied, dass der Host-Provider bei einer beanstandeten Bewertung auf einem Ärzteportal die Identität des Bewertenden nicht preisgeben muss, ihn dafür aber weitreichende Prüf- oder sogar Ermittlungspflichten treffen, findet sich in Österreich in § 18 E-Commerce-Gesetz (ECG) ein alternativer Ansatz. Der österreichische Gesetzgeber hat nämlich, über die Vorgaben der E-Commerce-Richtlinie hinausgehend, einen Auskunftsanspruch des Host-Providers gegenüber Dritten statuiert.

Nach § 18 Abs 4 ECG haben die in § 16 ECG genannten Diensteanbieter den Namen und die Adresse eines Nutzers ihres Dienstes, mit dem sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, unter bestimmten Voraussetzungen auf Verlangen dritten Personen zu übermitteln. Dies ist der Fall, wenn ein überwiegendes rechtliches Interesse an der Feststellung der Identität eines Nutzers und eines bestimmten rechtswidrigen Sachverhalts besteht sowie überdies glaubhaft gemacht werden kann, dass die Kenntnis dieser Informationen eine wesentliche Voraussetzung für die Rechtsverfolgung bildet.[13] Die dabei vorzunehmende Interessenabwägung wurde hier vom Gesetzgeber bereits vorgezeichnet.

Durch die genannte Bestimmung hat der Verletzte die Möglichkeit, direkt gegen den Verletzer vorzugehen. Damit kann eine Klage gegen den Host-Provider unter Umständen vermieden werden.[14] Ein überwiegendes rechtliches Interesse an der Feststellung der Identität besteht dabei dann, wenn die Rechtsverfolgung aufgrund einer groben Prüfung der vom Kläger geltend gemachten Verletzungen eine gewisse Aussicht auf Erfolg hat.[15]

10 Vgl *Thiele,* Die Trias von § 16 ABGB, § 78 UrhG und Datenschutz, in *Jahnel* (Hrsg), Datenschutzrecht (2015) 54 f.
11 Siehe FN 2.
12 Siehe nur das Urteil vom BGH 1. 3. 2016, VI ZR 34/15; vgl dazu *Hofmann*, Prozeduralisierung der Haftungsvoraussetzungen im Medienrecht, ZUM 2017, 102.
13 StRsp, siehe nur OGH 6 Ob 145/14 p JBl 2015, 448; 6 Ob 188/16 i MR 2017, 61.
14 *Ciresa* in *Schwimann/Kodek* (Hrsg), ABGB – Praxiskommentar[4] (2011) § 18 ECG Rz 16.
15 OGH 6 Ob 188/16 i MR 2017, 61.

Die Anforderungen an den Provider dürfen hier nicht überspannt werden. Die nach § 1330 ABGB im Einzelfall notwendige Grenzziehung zwischen Tatsachenbehauptung, Werturteil und Wertungsexzess ist damit bspw nicht im Auskunftsverfahren gegen den Betreiber der Website näher zu prüfen, sondern erst im Verfahren gegen den konkreten Poster. Voraussetzung ist lediglich, dass aufgrund einer groben Prüfung der vom Kläger geltend gemachten Verletzungen eine Verurteilung nach § 1330 ABGB nicht gänzlich auszuschließen ist.[16]

Freilich kann der Auskunftsanspruch nach § 18 ECG in der Praxis daran scheitern, dass der Provider keine Informationen über den Namen und die Anschrift des Verletzers hat. Rechtlich kann der Anspruch etwa dann scheitern, wenn andere Rechte, etwa das Redaktionsgeheimnis,[17] schwerer wiegen.[18]

IV. Ausblick

Die angesprochenen Themen und Fragen sind juristisch noch längst nicht erschöpfend behandelt oder ausjudiziert. Vielmehr stellen sich immer neue Fragen im digitalen Umfeld. Ein Beispiel dafür ist der sog „digitale Nachlass" einer Person. Was passiert etwa nach dem Tod einer Person mit ihren Accounts in sozialen Netzwerken („digitale Spuren")?[19] Diese enthalten regelmäßig höchstpersönliche Inhalte und sind in der analogen Welt wohl mit Tagebüchern und Briefen vergleichbar, wenngleich aus ihnen häufig sogar noch mehr über eine Person in Erfahrung gebracht werden kann. Inwieweit und von wem sind hier datenschutzrechtliche und persönlichkeitsrechtliche Interessen der verstorbenen Person zu berücksichtigen und zu wahren? Wer hat Ansprüche auf Herausgabe von Daten gegenüber dem sozialen Netzwerk? Muss die verstorbene Person zu Lebzeiten aktiv werden, um solche Ansprüche auszuschließen?

In besonders drastischer Weise zeigt sich diese Problematik in einem aktuellen Fall[20] in Deutschland: Eine Mutter wollte auf das Facebook-Konto ihrer verstorbenen minderjährigen Tochter zugreifen, die mutmaßlich Selbstmord begangen hatte (sie wurde von einer U-Bahn überfahren). Die verzweifelte Mutter erhoffte sich dadurch Aufschlüsse über die möglichen Beweggründe für diese Tat. Die Onlineplattform Facebook verweigerte die Herausgabe der Kontodaten und den Zugriff auf das Profil der verstorbenen Tochter, ua mit Hinweis auf den Datenschutz. Von der begehrten Offenlegung der Nachrichten seien darüber hinaus auch andere Nutzer betroffen. Das Gericht erster Instanz entschied, dass das Nutzerprofil der Tochter Teil des Erbes sei und die Eltern Anspruch auf Zugang haben. Das Gericht zweiter Instanz[21] entschied – noch nicht rechtskräftig – hingegen zugunsten von Facebook. Der Schutz des Fernmeldegeheimnisses stehe dem Anspruch der Erben entgegen, Einsicht in die Kommunikation der Tochter mit Dritten zu erhalten. Die Revision zum BGH wurde zugelassen. Die endgültige Entscheidung wird naturgemäß mit großem Interesse erwartet.

Zum Urteil der zweiten Instanz kann an dieser Stelle nur kurz angemerkt werden, dass die ausschließliche Stützung auf das Fernmeldegeheimnis, insb angesichts der besonders tragischen

16 Siehe RIS-Justiz RS0129335; zB OGH 6 Ob 133/13 x MR 2014, 59.
17 Vgl RIS-Justiz RS0129334; zB OGH 6 Ob 133/13x MR 2014, 59.
18 Probleme haben sich in der Vergangenheit auch iZm dynamischen IP-Adressen und deren Einordnung als Verkehrsdaten ergeben, siehe RIS-Justiz RS0124954.
19 Vgl dazu zB *Brehm*, Ausgewählte Fragen zum Umgang mit dem digitalen Nachlass, JEV 2016, 159.
20 LG Berlin 20 O 172/15 DNotZ 2016, 537.
21 KG 21 U 9/16 BeckRS 2017, 111509.

Umstände, nicht restlos nachvollziehbar erscheint. Weder wurde die Eltern-Kind-Beziehung, noch die Minderjährigkeit, noch wurden die Persönlichkeitsrechte des verstorbenen Mädchens berücksichtigt. Fraglich ist, ob in einem solchen Ausnahmefall nicht vielmehr eine Abwägung der verschiedenen betroffenen Rechte angebracht wäre, weil weder der Datenschutz noch das Fernmeldegeheimnis als absolut anzusehen sind. Auch in der analogen Welt wäre ein Auskunfts- oder Herausgabeanspruch gegen Dritte im Hinblick auf Informationen, die den vermeintlichen Selbstmord eines minderjährigen Kindes aufklären können, denkbar. In Österreich wurde – soweit ersichtlich – bislang noch kein derartiger Fall vor Gericht gebracht. Es ist aber offensichtlich, dass diese Fragen in Zukunft auch andere europäische Gerichte beschäftigen werden.

Viele neue Fragen werden sich schließlich spätestens ab dem 25. 5. 2018 auch durch die neuen Vorgaben der DSGVO stellen. Die bestehenden gesetzlichen Bestimmungen müssen einer gründlichen legistischen Prüfung auf ihre Vereinbarkeit mit der (unmittelbar anwendbaren) Verordnung unterzogen werden. Darüber hinaus sind die nationalen Gesetzgeber an einigen Stellen der Verordnung durch sog Öffnungsklauseln dazu ermächtigt, die Regelungen der Verordnung zu konkretisieren oder zu ergänzen. Auf die Ergebnisse und die verschiedenen Reaktionen der Mitgliedstaaten darf mit Interesse gewartet werden.

AUSTRIAN LAW JOURNAL

ISSN: 2409-6911

DOI: 10.25364/1.4:2017.2.6
www.austrian-law-journal.at

Cyber Crime – Der digitalisierte Täter

Susanne Reindl-Krauskopf[*], Universität Wien

Kurztext: *„Smart Home: Hacker übernehmen Kontrolle über Thermostat",[1] „Medjacking – Attacke auf Herzschrittmacher",[2] „Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid",[3] „Ransomware: Erpressung per Lösegeld-Trojaner",[4] „Tesla's Self-Driving System Cleared in Deadly Crash."[5]*

Schlagzeilen wie diese beschreiben den digitalisierten Täter der heutigen Zeit. Die Liste der Beispiele an modernen Straftaten lässt sich zwanglos erweitern durch Phänomene wie Online-Pornographie, Online-Glückspiel und Geldwäsche, digitale Erpressung, Cybermobbing und überhaupt Hate speech im Internet oder durch Eingriffe in die Privatsphäre über das Internet.[6]

Wie stets, wenn der technische Fortschritt für den Einzelnen und die Gesellschaft Vorteile bringt, zeigt sich auch bei der fortschreitenden Digitalisierung die Kehrseite der Medaille, nämlich der Kriminelle, der die neu eröffneten Möglichkeiten zu verpönten Zwecken nutzt. Was der solcherart digitalisierte Täter für das gerichtliche Strafrecht bedeutet, möchte ich im Folgenden exemplarisch beleuchten.

Schlagworte: *Cyber Crime, Hacking, Smart Home, digitale Erpressung, Smart Car.*

I. Smart Home gehackt – Eigentümer frierend gefangen

Ausgangsbeispiel: X bewohnt ein sog Smart Home. Das Smart-Home-System steuert alles, was man so braucht. Die Strom- und Wasserzufuhr wird „smart" an die analysierten Bedürfnisse des Nutzers angepasst, der Lebensmitteleinkauf durch den Kühlschrank automatisch geplant und durchgeführt usw. Ua werden auch das Heizungs- und das Sicherheitssystem intelligent gesteuert. Zu diesem Smart Home System verschafft sich der Täter Zugriff, indem er Sicherheitsvorkehrungen

* Univ.-Prof. Hon.-Prof. Dr. *Susanne Reindl-Krauskopf* ist Universitätsprofessorin am Institut für Strafrecht der Universität Wien.

1 https://www.heise.de/newsticker/meldung/Smart-Home-Hacker-uebernehmen-Kontrolle-ueber-Thermostat-3291209.html (abgefragt am 17. 3. 2017).

2 http://www.tagesanzeiger.ch/sonntagszeitung/Attacke-auf-den-Herzschrittmacher/story/28372909 (abgefragt am 22. 3. 2017).

3 https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (abgefragt am 20. 3. 2017).

4 http://www.computerbetrug.de/ransomware-erpressung-per-losegeld-trojaner (abgefragt am 22. 3. 2017).

5 https://www.nytimes.com/2017/01/19/business/tesla-model-s-autopilot-fatal-crash.html?_r=0 (abgefragt am 17. 3. 2017).

6 http://www.ubergizmo.com/2017/02/smart-teddy-bear-leaks-recordings/ (abgefragt am 22. 3. 2017), wonach mittels internettauglicher Bestandteile von Teddybären geheim Aufnahmen von Eltern und Kindern angefertigt und verbreitet worden sein sollen.

im System knackt. Einmal ins System vorgedrungen, manipuliert er es derart, dass die Heizung abgeschalten und der Sperrmechanismus verschlossen wird. X ist aufgrund der Manipulation durch den Täter nicht in der Lage, wieder Kontrolle über Heiz- und Sicherheitssystem zu erlangen. Er muss stundenlang im Dunkeln und in der Kälte ausharren.

Betrachtet man dieses Beispiel aus strafrechtlicher Sicht, so wird schnell deutlich, dass es um zwei Komplexe geht: zum einen um das Knacken des Systems und zum anderen um das Gefangenhalten und Frierenlassen.

A. Systemhack

Für das Eindringen in fremde Computersysteme sieht das Strafrecht als spezifisches Delikt seit 2002[7] den widerrechtlichen Zugriff auf ein Computersystem nach § 118a StGB vor.

§ 118a Abs 1 StGB idF StRÄG 2015:[8]

> *„Wer sich zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen durch Überwindung einer spezifischen Sicherheitsvorkehrung im Computersystem in der Absicht Zugang verschafft,*
>
> *1. sich oder einem anderen Unbefugten Kenntnis von personenbezogenen Daten zu verschaffen, deren Kenntnis schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt, oder*
> *2. einem anderen durch die Verwendung von im System gespeicherten und nicht für ihn bestimmten Daten, deren Kenntnis er sich verschafft, oder durch die Verwendung des Computersystems einen Nachteil zuzufügen,*
>
> *ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen."*

Nach der Kurzbeschreibung des Beispiels könnte der Täter durchaus entsprechend dem objektiven Tatbestand handeln: Da Computersystem jede einzelne oder verbundene Einrichtung ist, die der Datenverarbeitung dient, ist auch das vernetzte intelligente Zuhause, in dem die verschiedenen Funktionen durch miteinander verbundene Datenverarbeitungseinrichtungen gesteuert werden, ein Computersystem im Sinne der Legaldefinition des § 74 Abs 1 Z 8 StGB[9] und damit Tatobjekt des § 118a StGB. Der Täter hat im Beispiel keine rechtmäßige Verbindung zum Smart Home, er ist offenkundig weder Eigentümer noch Nutzungsberechtigter. Daher greift er auf ein Computersystem zu, über das er nicht allein verfügungsbefugt ist.[10] Dringt der Täter durch Überwinden von spezifischen Sicherheitsvorkehrungen in dieses System ein, so hat er den objektiven Tatbestand verwirklicht. Nachdem die Formulierung im Beispiel darauf abstellt, dass das System geknackt wurde, ist davon auszugehen, dass der Täter tatsächlich Sicherheitsvorkehrungen ausgeschaltet

7 BGBl I 2002/134.

8 BGBl I 2015/112.

9 Näher zur Frage, welche Einrichtungen als Computersystem in diesem Sinne in Frage kommen, siehe ua bei *Bergauer*, Das materielle Computerstrafrecht (2016) 75 ff*; Fabrizy*, StGB[12] § 74 Rz 25; *Tipold* in *Leukauf/Steininger*, StGB[4] § 74 Rz 33; *Nittel* in *Triffterer/Rosbaud/Hinterhofer*, SbgK StGB[36] § 74 Rz 143 ff; *Reindl-Krauskopf* in *Höpfel/Ratz*, WK[2] StGB (166. Lfg 2017) § 74 Abs 1 Z 8 insb Rz 58; *dies* in *Höpfel/Ratz*, WK[2] StGB (117. Lfg 2014) § 118a Rz 6–9.

10 Zur Verfügungsbefugnis siehe *Bergauer,* Computerstrafrecht 84 f*; Birklbauer/Hilf/Tipold,* Strafrecht BT I[3] § 118a Rz 3; *Fuchs/Reindl-Krauskopf*, Strafrecht BT I[5] 128; *Tipold* in *Leukauf/Steininger,* StGB[4] § 118a Rz 2; *Reindl-Krauskopf* in *Höpfel/Ratz*, WK[2] StGB (117. Lfg 2014) § 118a Rz 10–18; *Thiele* in *Triffterer/Rosbaud/Hinterhofer*, SbgK StGB[36] § 118a Rz 31 f.

hat,[11] um in das System vordringen zu können, was dem Erfordernis des Überwindens einer Sicherheitsvorkehrung jedenfalls entspricht.[12] Ungesicherte[13] Systeme werden demgegenüber von § 118a StGB nicht geschützt.[14]

Damit alleine ist es allerdings noch nicht getan. Um tatsächlich nach § 118a StGB strafbar zu sein, muss der Täter auch mit einem besonderen Vorsatz[15] handeln. Zum einen muss er es ernstlich für möglich halten und sich damit abfinden, dass er unter Überwindung von spezifischen Sicherheitsvorkehrungen in ein Computersystem eindringt, über das er nicht allein verfügungsberechtigt ist. Zum anderen braucht er aber auch eine zusätzliche Absicht. Diese kann sich seit dem StRÄG 2015 nunmehr alternativ auf drei unterschiedliche Aspekte beziehen:[16] Entweder kommt es dem Täter darauf an, sich oder einem anderen Unbefugten Kenntnis von personenbezogenen Daten zu verschaffen, deren Kenntnis schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt, oder es kommt ihm darauf an, einem anderen durch die Verwendung von im System gespeicherten und nicht für ihn bestimmten Daten, deren Kenntnis er sich verschafft, einen Nachteil zuzufügen. Schließlich kommt als dritte Alternative die Absicht in Frage, einem anderen durch die Verwendung des Computersystems selbst einen Nachteil zuzufügen. Der vom Tatbestand angesprochene Nachteil muss übrigens keineswegs finanzieller Natur sein, vielmehr kommen Nachteile jeder Art in Frage,[17] also etwa auch die Beeinträchtigung der Gesundheit, Freiheit und der Privatsphäre.

Im vorliegenden Fall geht es dem Täter offensichtlich darum, durch die Manipulation des Systems die Heizung abzudrehen sowie den Sperrmechanismus zu verschließen und den Bewohner frierend gefangen zu halten. In der Manipulation des Systems zu diesem Zweck liegt eine Verwen-

11 Wurden dafür spezielle Computerprogramme verwendet, die nach ihrer besonderen Beschaffenheit ersichtlich gerade zur Begehung des widerrechtlichen Zugriffs auf ein Computersystem iSd § 118a StGB hergestellt wurden, so kann bereits im Vorfeld zum eigentlichen Zugriff auf das System eine Strafbarkeit nach § 126c StGB (Missbrauch von Computerprogrammen und Zugangsdaten) bestehen. Diese kann ua den Hersteller, Veräußerer und Besitzer solcher Programme treffen. Näher zu § 126c StGB siehe nur ua *Bergauer,* Computerstrafrecht 317 ff; *Reindl-Krauskopf* in *Höpfel/Ratz*, WK^2 StGB (3 (A) Lfg 2008) § 126c.

12 Zur Streitfrage, ob das Umgehen von Sicherheitsvorkehrungen bereits ein Überwinden sein kann, siehe grundsätzlich befürwortend, sofern ein vorhandenes Sicherheitssystem aufgrund der Manipulation des Täters nicht aktiviert wird, *Reindl-Krauskopf* in *Höpfel/Ratz*, WK^2 StGB (117. Lfg 2014) § 118a Rz 26 ff; aA *Bergauer,* Computerstrafrecht 100–104, dessen Vergleich mit dem Kurzschließen eines PKW aber insofern fehlgeht, als es beim Einbruchsdiebstahl weder um das Überwinden noch um das Umgehen einer Sicherung, sondern um das Aufbrechen einer Sperrvorrichtung geht und die Judikatur daher die Frage, ob das Kurzschließen ein Umgehen oder ein Überwinden ist, nicht zu beurteilen hatte; bleibt nur abschließend anzumerken, dass ein Aufbrechen einer Sperrvorrichtung ein Aliud sowohl zum Überwinden wie auch zum Umgehen einer Sicherung ist.

13 Zu den Anforderungen an die spezifische Sicherung siehe ua *Bergauer,* Computerstrafrecht 89*; Fabrizy,* StGB^{12} § 118a Rz 3; *Fuchs/Reindl-Krauskopf*, Strafrecht BT I^5 128; *Tipold* in *Leukauf/Steininger,* StGB^4 § 118a Rz 5; *Reindl-Krauskopf* in *Höpfel/Ratz*, WK^2 StGB (117. Lfg 2014) § 118a Rz 25; *Thiele* in *Triffterer/Rosbaud/Hinterhofer,* SbgK StGB^{36} § 118a Rz 37 ff.

14 So explizit ua auch *Seling,* Schutz der Privatsphäre durch das Strafrecht (2010) 77.

15 *Bertel/Schwaighofer/Venier*, Österreichisches Strafrecht BT I^{13} § 118a Rz 3; *Fuchs/Reindl-Krauskopf*, Strafrecht BT I^5 129.

16 Zuvor verlangte der Tatbestand die Absicht des Täters, sich oder einem anderen Unbefugten von in einem Computersystem gespeicherten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen. Diese hohe Anforderung an den subjektiven Tatbestand führte zur Straflosigkeit verschiedener Fallkonstellationen und damit zu unbefriedigenden Ergebnissen (siehe dazu nur *Bergauer,* Computerstrafrecht 104 ff*; Reindl-Krauskopf* in *Höpfel/Ratz*, WK^2 StGB (117. Lfg 2014) § 118a Rz 34–38; *Salimi,* Zahnloses Cyberstrafrecht? ÖJZ 2012, 998 (999 f); *Seling,* Schutz 78 ff.

17 Zum Begriff des Nachteils in diesem Zusammenhang siehe ua *Reindl-Krauskopf* in *Höpfel/Ratz*, WK^2 StGB (117. Lfg 2014) § 118a Rz 37; *Thiele* in *Triffterer/Rosbaud/Hinterhofer*, SbgK StGB^{36} § 118a Rz 68.

dung des Computersystems, denn als Verwendung ist jede Nutzung anzusehen. Dass es sich beim Frieren und bei der Unmöglichkeit, das Haus zu verlassen, um Nachteile für den Bewohner handelt, die durch die Verwendung des Systems bewirkt werden, liegt auf der Hand. Der Täter in diesem Beispiel erfüllt somit auch die Anforderungen des subjektiven Tatbestandes.[18] Schon durch das Eindringen in das Smart Home erfüllt der digitalisierte Täter somit den strafrechtlichen Tatbestand des § 118a StGB. Daneben könnte freilich abhängig von der technischen Vorgehensweise beim Eindringen uU auch eine Datenbeschädigung nach § 126a StGB gegeben sein.[19] Die Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB) ist hingegen im Zusammenhang mit der Manipulation des Systems wohl eher zu verneinen, weil das System als solches nicht gestört ist.[20] Es kann bloß im Moment ausschließlich vom Täter genutzt werden. Diese Aspekte sollen hier aber nicht weiter vertieft werden.

B. Weitere Folgen

Im Ausgangsbeispiel wird der Bewohner frierend gefangen gehalten. Damit bewegt sich der digitalisierte Täter wieder im Bereich klassischer Delikte; es geht nämlich um Freiheitsentziehung nach § 99 StGB. Je nach Ausmaß und gesundheitlichen Folgen des Frierens könnte man auch noch an die Delikte zum Schutz von Leib und Leben denken. An der diesbezüglichen Verantwortlichkeit ändert auch die digitalisierte Begehungsweise nichts.

Der Täter des Ausgangsbeispiels könnte das geknackte Smart Home System natürlich auch für ganz andere Dinge nutzen. Intelligente Systeme können schließlich nur im beschriebenen Sinn funktionieren, wenn sie viele Daten über den Nutzer sammeln. Nur wenn die Systeme die Lebensgewohnheiten ihres Nutzers abbilden, wird zur richtigen Zeit die Stromzufuhr gestartet oder gedrosselt, die Tür ver- oder entsperrt etc. Der Täter kann das System folglich auch nutzen, um personenbezogene Informationen über sein Opfer zu sammeln. Abgesehen vom Eindringen in das System wäre das strafrechtlich noch nicht relevant. Nutzt der Täter diese Informationen allerdings für einen Einbruch, weil er nach dem Studium der Lebensgewohnheiten weiß, wann sein Opfer nicht zu Hause sein wird, so schließt an die Strafbarkeit wegen des Widerrechtlichen Zugriffs auf ein Computersystem eine mögliche Strafbarkeit wegen des Einbruchsdiebstahls nach §§ 127, 129 StGB ebenso wie wegen Datenverwendung in Gewinn- oder Schädigungsabsicht nach § 51 DSG[21] an. Allerdings wäre § 51 DSG in einer solchen Konstellation aufgrund des expliziten Gesetzeswortlautes nur subsidiär anwendbar. Die ausspionierten personenbezogenen Daten lassen sich aber selbstverständlich auch anders, zB zu Erpressungen, kriminell nutzen.

Die Digitalisierung des Täters führt im Ausgangsbeispiel und diesen vergleichbaren Fällen zu keinen besonderen neuen Herausforderungen für das materielle Strafrecht. Das Phänomen des gehackten Smart Home zeigt aber deutlich, wie ganz traditionelle Ziele des Täters, nämlich etwa

18 Bis zum StRÄG 2015 wäre dieser Fall allerdings nicht von § 118a StGB erfasst worden, weil der subjektive Tatbestand wesentlich mehr Anforderungen enthielt.

19 Zur Datenbeschädigung iSd § 126a StGB allgemein: *Bergauer,* Computerstrafrecht 237 ff*; Bertel* in *Höpfel/Ratz*, WK^2 StGB (3 (A) Lfg 2008) § 126a; *Komenda/Madl* in *Triffterer/Rosbaud/Hinterhofer*, SbgK StGB^{36} § 126a; *Messner* in *Leukauf/Steininger*, StGB^4 § 126a.

20 Allgemein zu diesem Delikt *Bergauer,* Computerstrafrecht 287 ff; *Daxecker* in *Triffterer/Rosbaud/Hinterhofer*, SbgK StGB^{36} § 126b; *Messner* in *Leukauf/Steininger,* StGB^4 § 126b; *Öhlböck/Esztegar*, Rechtliche Qualifikation von Denial of Service Attacken, JSt 2011, 126; *Reindl-Krauskopf in Höpfel/Ratz*, WK^2 StGB (3 (A) Lfg 2008) § 126b.

21 Zu § 51 DSG siehe näher nur *Bergauer*, Computerstrafrecht 117 ff; *Salimi* in *Höpfel/Ratz*, WK^2 StGB (84. Lfg 2012) § 51 DSG.

die Entziehung der Freiheit des Opfers, auch mit digitalisierten Handlungsweisen verwirklicht werden können.

II. Medjacking – Attacke auf Herzschrittmacher

Ausgangsbeispiel: Y ist auf einen Herzschrittmacher angewiesen, der mit dem System des Krankenhauses vernetzt ist, in dem Y ständig behandelt wird. Der Täter knackt das System, um Y zu töten.

Die Vorgehensweise des Täters ist im Grunde vergleichbar mit dem ersten Beispiel. Auch hier nutzt er die Vernetzung der Systeme aus, dringt in ein Computersystem ein und manipuliert dieses. Die mögliche Konsequenz wiegt aber wesentlich schwerer und reicht von der bloßen Gefährdung des Patienten bis hin zu seinem Tod.

Solche Attacken sind nicht bloß bei Herzschrittmachern vorstellbar. Bei Medizinprodukten besteht ein allgemeiner Trend hin zum Hightech-Produkt, etwa auch bei Insulinpumpen oder Hirnelektroden.[22] Auch solche medizinische Hilfsmittel arbeiten auf Basis der Vernetzung und reagieren abgestimmt auf und angepasst an den Bedarf des Patienten. Manipuliert sie der digitalisierte Täter, nachdem er sich Zugang zu den relevanten Systemen verschafft hat, kann der betreffende Patient vom Täter zB aufgrund einer im System herbeigeführten Verabreichung einer Überdosis an Insulin getötet werden.

Dass der Täter diesfalls für die verursachten Körperverletzungs- und Tötungsdelikte verantwortlich ist, steht außer Frage, weil es für die Strafbarkeit auf die technische Art und Weise der Herbeiführung einer Körperverletzung oder Tötung nicht ankommt. Die relevanten Delikte sind nämlich als Erfolgsverursachungsdelikte[23] und somit technikneutral konzipiert.

Es stellt sich aber wieder die zusätzliche Frage, ob bereits das Eindringen in das System strafrechtlich relevant sein kann, ob also strafrechtliche Verantwortung spruchreif wird, bevor überhaupt noch eine Gesundheitsgefahr entsteht. In Frage kommt wieder § 118a StGB. Der Täter verschafft sich Zugang zu einem Computersystem, über das er typischerweise nicht allein verfügungsbefugt ist. Er handelt im Ausgangsbeispiel auch in der Absicht, durch Verwendung des Computersystems dem betroffenen Patienten einen Nachteil zuzufügen; er will ihn ja töten.[24]

Ob § 118a StGB allerdings tatsächlich bereits im Vorfeld greift, wird oftmals davon abhängen, auf welche technische Art und Weise der Zugriff auf das Computersystem erlangt wird. Immer wieder wird nämlich berichtet, dass Zugriffe aufgrund von Sicherheitslücken möglich sind.[25] Nutzt der Täter allgemein bekannte Lücken aus und muss er daher für die Erlangung des widerrechtlichen Zugriffs auf das Computersystem gar keine besondere kriminelle Energie aufbringen, dann scheitert die Anwendung des § 118a StGB idR. Denn dann überwindet er bei seinem Zugriff nicht – wie

22 Ua http://www.tagesanzeiger.ch/sonntagszeitung/Attacke-auf-den-Herzschrittmacher/story/28372909 (abgefragt am 22. 3. 2017).

23 Zu diesem Begriff statt vieler *Fuchs,* Strafrecht AT I[9] Kap 10/41.

24 Denkbar sind freilich auch Fälle, in denen der Täter die Absicht hat, die jeweilige medizinische Einrichtung, die ein solches System betreibt, oder den Hersteller des betreffenden Medizinproduktes mit Geldforderungen zu konfrontieren und für den Fall der Zahlungsverweigerung mit der Schädigung des Patienten zu drohen.

25 Ua http://www.tagesanzeiger.ch/sonntagszeitung/Attacke-auf-den-Herzschrittmacher/story/28372909 (abgefragt am 22. 3. 2017).

vom Tatbestand gefordert – spezifische Sicherheitsvorkehrungen im System.[26] Er bleibt aus dem Blickwinkel des § 118a StGB straflos.

Das mag auf den ersten Blick irritieren, zumal es in dieser Konstellation um in weiterer Folge lebensbedrohliche Angriffe seitens des digitalisierten Täters geht. Doch ist das Gesetz hier durchaus konsequent. Deutlich wird dies etwa bei dem Vergleich mit dem Hausfriedensbruch.[27] Der bloß unbefugte Eintritt in eine fremde Wohnung durch eine offenstehende Türe ist als solcher kein Fall für das Strafrecht; auch nicht, wenn der Eindringling im Anschluss daran den Wohnungseigentümer ermordet. Der Mord bleibt als vorsätzliche Tötung eines Menschen selbstverständlich strafbar. Dasselbe gilt konsequenterweise auch für den digitalisierten Eindringling, der in weiterer Folge den Patienten durch Manipulation des Herzschrittmachers oder der Insulinpumpe vorsätzlich tötet: Das Eindringen in das System durch die offenstehende digitale „Tür" bleibt straflos, die nachfolgende vorsätzliche Tötung strafbar.

In Frage könnte für eine allfällige Beschädigung von Daten beim Eindringen ins System und für die weitere Manipulation im System uU aber auch in solchen Fällen wieder die Datenbeschädigung iSd § 126a StGB kommen.

Auch Fälle wie dieses zweite Beispiel werfen letztlich keine gänzlich neuen Fragen für das Strafrecht auf. Allerdings muss sich die Gesellschaft rasch der neuen kriminellen Werkzeuge und Handlungsformen bewusst werden, um sich vor Attacken schützen zu können. Dazu gehört ua auch die Bewusstseinsbildung dahingehend, bei welchen Computersystemen welche Sicherheitsrisiken und Anfälligkeiten bestehen und welche Sicherheitsstandards für bestimmte Anwendungen daher unbedingt einzuhalten sind. Das betrifft allerdings die Vorbeugung von Rechtsgutsbedrohungen und Verletzungen schon weit im Vorfeld allfälliger strafrechtlicher Fragen.

III. Digitale Erpressung

Fälle der digitalen Erpressung wurden der österreichischen Öffentlichkeit va durch den sog „Polizei-Trojaner"[28] bekannt. Dabei wurde der PC des Opfers zunächst mit einem Schadprogramm infiziert, das sich beim nächsten Starten des PC aktivierte. Am Bildschirm erschien dann die Mitteilung, dass der PC wegen angeblich auf dem PC gespeicherten strafrechtlich relevanten, zB kinderpornographischen, Materials von der Polizei gesperrt worden sei. Um die Echtheit der Mitteilung zu unterstreichen wurde das täuschend echte Logo der österreichischen Polizei verwendet. Das Opfer wurde nun darüber informiert, dass die Sperre erst nach Bezahlung eines Strafbetrages aufgehoben wird.[29]

Beurteilt man dieses Szenario aus strafrechtlicher Sicht, so ist zwischen dem Kapern des PC und der Geldforderung im Gegenzug zur Entsperrung des PC zu unterscheiden. Je nach technischer Vorgehensweise könnte auch hier für den ersten Tatkomplex, also für das Infiltrieren des PC mit der Schadsoftware, wieder an § 118a StGB zu denken sein. Voraussetzung ist freilich wieder, dass der Täter beim Einschleusen des Schadprogrammes eine spezifische Sicherheitsvorkehrung im

26 *Reindl-Krauskopf* in *Höpfel/Ratz*, WK² StGB (117. Lfg 2014) § 118a Rz 29; tendenziell enger *Bergauer,* Computerstrafrecht 88–104.

27 § 109 StGB.

28 Zum Ganzen insb Cybercrime-Report des ö BK 2012, 12; Cybercrime Bundeslagebild des dt BKA 2012, 7.

29 Siehe dazu auch *Reindl-Krauskopf*, Cyberstrafrecht im Wandel, ÖJZ 2015, 112 (112 f).

System überwindet. Tut er dies, so liegt eine Strafbarkeit nach § 118a StGB sehr nahe. Denn er handelt typischerweise auch in der Absicht, durch Verwendung des infiltrierten Computersystems dem berechtigten Nutzer einen Nachteil zuzufügen. Überwindet der Täter hingegen keine spezifische Sicherheitsvorkehrung, so scheidet eine Strafbarkeit nach § 118a StGB von Vornherein aus.

Beschädigt der Täter beim Installieren des Schadprogramms vermögenswerte Daten am PC des Opfers, so kann zumindest der Schutz der Datenbeschädigung nach § 126a StGB greifen. Ist aber auch das nicht der Fall, so bleibt das unbefugte Eindringen in das fremde Computersystem und das Infiltrieren mit dem Schadprogramm ohne strafrechtlichen Schutz. Erst die Tatsache, dass das Opfer sein System wegen der Sperre nicht nutzen kann, wird strafrechtlich relevant. Durch die softwaremäßige Sperre hindert der Täter das Opfer nämlich am Zugang zu den eigenen Daten. Da diese typischerweise zumindest Gebrauchswert haben werden, unterdrückt der Täter daher idR von § 126a StGB geschützte Daten in strafbarer Weise.[30]

Keine Beurteilungsschwierigkeiten bereitet hingegen nach der hM die Forderung des Täters, Geld im Gegenzug für die Aufhebung der Sperre zu bezahlen. Der Täter droht dem Opfer damit, den Gebrauch des PC weiterhin zu verhindern, also das Vermögen des Opfers weiter zu verletzen, und nötigt es so zur Zahlung einer gewissen Summe. Da die Aufhebung der Sperre im Gegenzug zur Zahlung keine anrechenbare Gegenleistung ist, weil nur etwas geschieht, worauf der am PC Berechtigte ohnedies einen begründeten Anspruch hat, geht die hM in vergleichbaren Fällen vom Vorliegen einer Erpressung nach § 144 StGB aus.[31] Folgte man hier der Mindermeinung, wäre die Schädigung des Betroffenen bereits mit der Sperre des PC eingetreten und die weitere Forderung bestenfalls noch als Nötigung strafrechtlich relevant.[32] Haben die Täter allerdings gar nicht vor, die Sperre für den Fall der Zahlung des „Lösegeldes" tatsächlich aufzuheben, wäre auch an eine Strafbarkeit wegen Betruges zu denken. Auch bei dieser Fallkonstellation bewegt sich der digitalisierte Täter somit letztlich im klassischen Strafrecht.

IV. Smart Cars und Unfälle

Abschließend noch zu einem Beispiel aus dem Fahrlässigkeitsbereich, nämlich Smart Cars und Verkehrsunfällen. Intelligente Autos sollen uns ua helfen, Sicherheitsrisiken rechtzeitig zu erkennen, uns vor Staus warnen usw. Nun ist es zwar denkbar, dass auch solche Autos bewusst dazu missbraucht werden, um zB eine Massenkarambolage herbeizuführen. Spannender erscheint mir aber die Frage, wie mit nicht vorsätzlichem Fehlverhalten umzugehen ist.

Intelligente Systeme in Autos wie zB Einparkhilfen können uns nur deshalb beim Fahren unterstützen, weil sie durch Sensoren Umweltdaten aufnehmen, Abstände messen, Geschwindigkeiten anpassen etc. Funktioniert ein solches System nicht oder fällt es aus und kommt es deshalb zu

30 Die Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB) ist hingegen wohl wieder zu verneinen, weil das System als solches nicht gestört ist. Es kann bloß im Moment ausschließlich vom Täter genutzt werden.

31 Zur vergleichbaren Konstellation der „Kunsterpressung" siehe OGH 11 Os 3/07m SSt 2007/11 = EvBl 2007/86 = JBl 2008, 198 (krit *Schmoller*); *Eder-Rieder* in *Höpfel/Ratz*, WK^2 StGB (138. Lfg 2016) § 144 Rz 27; *Fabrizy*, StGB^{12} § 144 Rz 3; *Hintersteininger* in *Triffterer/Rosbaud/Hinterhofer*, SbgK StGB^{36} § 144 Rz 33; *Lewisch,* Strafrecht BT I^2 (2006) 222.

32 IdS *Schmoller* in *Kienapfel/Schmoller* (Hrsg), Studienbuch Strafrecht BT II (2003) § 144 Rz 44; auch die Nötigung verneinend *Flora* in *Leukauf/Steininger*, StGB^4 § 144 Rz 9; *Venier*, „Kunsterpressung" – ein vermögensstrafrechtliches Paradoxon? JSt 2004, 73 ff (insb 74–76).

einem Unfall mit Personenschaden, stellt sich die Frage nach der Strafbarkeit.[33] Dabei denkt man unweigerlich an die Fahrlässigkeitsdelikte nach §§ 80, 81 und 88 StGB. Wie bei jedem Fahrlässigkeitsdelikt stellt sich auch in der Konstellation des Smart Car die Frage nach einer objektiven Sorgfaltswidrigkeit.[34] In der derzeitigen Situation wäre zunächst an die Pflichten des Lenkers zu denken. Dabei sieht auch die Sonderregel des § 102 Abs 3b KFG[35] für Fahrzeuge mit Assistenzsystemen bzw automatisierten oder vernetzten Fahrsystemen vor, dass der Lenker seine Fahraufgaben jederzeit wieder zu übernehmen hat, wenn dies notwendig wird. Ist also objektiv erkennbar, dass ein Systemfehler auftritt, muss der Lenker eingreifen. Tut er nichts, ist seine Untätigkeit objektiv sorgfaltswidrig. Seine Strafbarkeit kann in der Folge problemlos anhand der allgemeinen Prinzipien der Fahrlässigkeitshaftung geprüft werden.

Zusätzlich wäre zu untersuchen, worin die Ursache des Systemfehlers lag. Ist bspw dem zuständigen Systembetreuer ein Wartungsfehler unterlaufen, so wäre trotz des Zusammenhangs mit einem intelligenten System nach wie vor von einer objektiven Sorgfaltswidrigkeit eines Menschen, eben dieses Systembetreuers auszugehen. Auch für ihn käme – wie ggf auch zB für den Hersteller und Programmierer solcher Systeme – nach den klassischen strafrechtlichen Prinzipien eine Haftung wegen eines Fahrlässigkeitsdeliktes in Frage. Freilich: Je autonomer das jeweilige Fahrsystem und je komplexer das Zusammenspiel technischer Komponenten, desto schwieriger kann sich mitunter der Nachweis der Kausalität des einzelnen Fehlverhaltens für den eingetretenen Erfolg gestalten. Aus strafrechtlicher Sicht reicht allerdings auch bloße Mitverursachung aus. Auf dem Stand der derzeitigen Technik erscheint das Strafrecht auch für den digitalisierten „Fahrlässigkeits-Täter" gerüstet.

Problematisch könnte das langfristig geplante Ziel der technischen Entwicklung sein, nämlich den menschlichen Lenker, der noch eingreifen kann, irgendwann vollständig zu ersetzen.[36] Dahinter steht die Überlegung, dass Maschinen anders als Menschen keine Fehler machen und damit deren Einsatz Unfälle drastisch reduzieren und die Verkehrssicherheit enorm steigern könnte. Kommt es dennoch zu Schädigungen anderer Verkehrsteilnehmer, stellt sich freilich trotzdem die Frage nach der strafrechtlichen Verantwortlichkeit; auch unabhängig von außerstrafrechtlichen und verschuldensunabhängigen Haftungen. Der Lenker kommt in einem solchen Szenario als strafrechtlich Verantwortlicher nicht mehr in Frage, weil er faktisch nicht mehr ins Geschehen eingreifen kann. Ist erfolgsabwendendes Verhalten *de facto* nicht möglich, scheidet die Strafbarkeit – zumindest auf Basis der heutigen Dogmatik – aus.[37] Geschah der Unfall aufgrund eines Herstellungs-, Programmierungs- oder Wartungsfehlers, so könnte sich als Anknüpfung für eine strafrechtliche Haftung freilich wieder ein objektiv sorgfaltswidriges Verhalten eines Herstellers, Programmierers oder Systembetreuers ergeben.[38]

---

33 Siehe zur Frage der strafrechtlichen Verantwortlichkeit nach österreichischem Recht insb auch *Rohregger*, Autonome Fahrzeuge und strafrechtliche Verantwortlichkeit, JSt 2017, 196.

34 Zu grundsätzlichen Fragen der Fahrlässigkeitsdogmatik iZm hochautomatisiertem Fahren siehe ua *Gless*, „Mein Auto fuhr zu schnell, nicht ich!" – Strafrechtliche Verantwortung für hochautomatisiertes Fahren, in *Gless/Seelmann* (Hrsg), Intelligente Agenten und das Recht (2016) 225; allgemein zu intelligenten Systemen ua *Gless/Weigend,* Intelligente Agenten und das Strafrecht, ZStW 2014, 561.

35 Eingeführt durch BGBl I 2016/67.

36 Siehe zu den unterschiedlichen Automatisierungsgraden ua *Hötitzsch/May,* Rechtliche Problemfelder beim Einsatz automatisierter Systeme im Straßenverkehr, in *Hilgendorf* (Hrsg), Robotik im Kontext von Recht und Moral (2014) 189.

37 HM siehe nur *Hilf* in *Höpfel/Ratz*, WK^2 StGB (59. Lfg 2005) § 2 Rz 46 mwN.

38 Dazu und zur Frage der Verantwortungsverlagerung vom Lenker auf andere Personen siehe für Österreich *Rohregger*, JSt 2017, 196 (199 f).

Es wird aber auch Konstellationen geben, in denen das System aus technischer Sicht nicht fehlerhaft gearbeitet hat und dennoch Menschen zu Schaden kommen:

A ist mit seinem autonom fahrenden Smart Car unterwegs, bei dem er nur mehr Passagier ist und aus technischer Sicht gar keine Möglichkeit mehr zum Eingreifen in den aktuellen Fahrvorgang hat. Ein Kind läuft vor dem Auto (unerwartet) auf die Straße. Ein Aufprall, bei dem das Kind wahrscheinlich zu Tode käme, könnte nur durch ein Ausweichmanöver erreicht werden, bei dem der Wagen allerdings gegen eine Mauer prallen und dadurch seinen Passagier A töten würde.

Würde ein Mensch in einer solchen Konstellation nicht ausweichen, um sich selbst zu retten, so könnte er zwar nie gerechtfertigt sein, weil sich in der Güterabwägung zwei gleichwertige Rechtsgüter, nämlich das Leben des ausweichenden Menschen und das Leben des Kindes, gegenüberstehen. Aber wegen des Verlangens, das eigene Leben zu retten, könnte der Mensch uU aufgrund entschuldigenden Notstandes nach § 10 StGB straflos werden. § 10 StGB setzt dafür nämlich eine gegenwärtige oder unmittelbar drohende Gefahr für ein Rechtsgut verbunden mit einer aktuellen psychischen Drucksituation beim Täter voraus; eine Höherwertigkeit des zu rettenden Rechtsgutes wird dabei nicht gefordert.[39] In einer solchen Situation bleibt das menschliche Verhalten zwar rechtswidrig, aber aufgrund des akuten Ausnahmezustandes, in dem der Mensch sich befindet, entfällt der Schuldvorwurf.

Das Smart Car kann einer vergleichbaren Drucksituation nicht ausgesetzt sein. Denn es trifft die Entscheidung nicht selbst, sondern die Reaktion muss vorweg für eine solche Situation programmiert werden. Diese Entscheidungen müssen also in einem Zeitpunkt getroffen werden, der weit vor dem eigentlichen Geschehen liegt. Damit stellt sich aus Sicht der Strafrechtsdogmatik die Frage, ob Entschuldigungsgründe auch denjenigen zugutekommen können, die die Entscheidung darüber treffen, wie das Smart Car für solche späteren Interessenskollisionen zu programmieren ist, oder ob traditionelle schuldausschließende Instrumente im Zusammenhang mit intelligenten Systemen für solche Interessenkollisionen schlicht unanwendbar sind. Denn immerhin wird die Entscheidung lange vor der eigentlichen akuten Unfallsituation getroffen. Auf Basis des derzeitigen Stands der Technik ergeben sich solche Konstellationen zwar noch nicht. Doch sollte sich die Strafrechtsdogmatik rechtzeitig solchen Herausforderungen stellen, um auch für die Zukunft befriedigende Lösungen für den Umgang mit digitalisierten Tätern bereit zu halten.

V. Conclusio

Mag die zuletzt aufgeworfene Fragestellung uU auch neue Überlegungen zur Strafrechtsdogmatik notwendig machen, so kann man doch nach derzeitigem Stand der technischen und rechtlichen Entwicklung festhalten, dass das Strafrecht – nicht zuletzt aufgrund der Anpassungen durch das StRÄG 2015 – im Großen und Ganzen auch für den digitalisierten Täter in den geschilderten Kriminalitätsbereichen gerüstet ist.

39 Zum entschuldigenden Notstand nach § 10 StGB und dessen Prinzipien *Fuchs*, Strafrecht AT I[9] Kap 24/8 ff; *Fabrizy*, StGB[12] § 10; *Höpfel in Höpfel/Ratz*, WK[2] StGB (22. Lfg 2012) § 10; *Kienapfel/Höpfel/Kert,* Lernprogramm Strafrecht AT I[15] (2016) Z 20; *Koller/Schütz* in *Leukauf/Steininger,* StGB[4] § 10; *Moos* in *Triffterer/Rosbaud/Hinterhofer*, SbgK StGB[36] § 10.

AUSTRIAN LAW JOURNAL

ISSN: 2409-6911

DOI: 10.25364/1.4:2017.2.7
www.austrian-law-journal.at

Cyber Crime – Der digitalisierte Täter

Christian Bergauer*, Universität Graz

***Kurztext**: Der vorliegende Kommentar bezieht sich auf den Beitrag „Cyber Crime – der digitalisierte Täter" von Susanne Reindl-Krauskopf (ALJ 2/2017, 110). Die Computerkriminalität ist aktuell wohl eines der am schnellsten wachsenden, aber auch unterschätztesten Kriminalitätsfelder und damit bereits zu einem massiven faktischen Problem in der Gesellschaft geworden. Allein im Jahr 2016 gab es in Österreich 13.103 Anzeigen wegen Cybercrime-Delikten.[1] Obwohl Cybercrime-Phänomene in allen Lebensbereichen zunehmen, sind sie noch nicht wirklich in der Rechtsprechung angekommen, was die äußerst wenigen Verurteilungszahlen bestätigen.[2] Dies beruht auf folgenden Gründen: Faktische Probleme der Täterausforschung in der informationstechnischen Umgebung, strafprozessuale Schwierigkeiten hinsichtlich IT-spezifischer Ermittlungsmaßnahmen insb bei Auslandsbezug und nicht zuletzt konzeptionell verbesserungsfähige Computerdelikte.[3]*

Die der Computerkriminalität zugrunde liegenden informationstechnischen Konzepte machen sie sehr facettenreich, weshalb die im Hauptvortrag von Reindl-Krauskopf diskutierten Phänomene lediglich eine kleine Auswahl an Erscheinungsformen der Computerkriminalität darstellen. In meinem Kommentar zu diesen Beispielsfällen, werde ich einige neue Herausforderungen für das Strafrecht dogmatisch sowie rechtspolitisch näher beleuchten.

***Schlagworte:** Cybercrime, Computerkriminalität, Computerstrafrecht, Hacking, Smart Cars, Ransomware, Medjacking*

Eingangs möchte ich mich bei den VeranstalterInnen für die Einladung bedanken, an dieser Tagung mit einem Kommentar zum Vortrag von Frau Univ.-Prof.in Dr.in *Susanne Reindl-Krauskopf* mitwirken zu dürfen. Der Mehrwert eines Kommentars liegt mE nicht in einem bloßen Resümee oder der besonderen Betonung jener Aspekte des Hauptvortrags, in denen ohnehin Einigkeit besteht (und solche gibt es viele), sondern insb in Ergänzungen und im Aufzeigen ggf etwas anders gelagerter Sichtweisen. So erlaube ich mir, einige ergänzende Bemerkungen zur dogmatischen Analyse von *Reindl-Krauskopf* ebenso wie einige rechtspolitische Gedanken zu einzelnen Themenberei-

* Az. Prof. Dr. *Christian Bergauer* ist assoziierter Professor am Institut für Rechtswissenschaftliche Grundlagen, Fachbereich Recht und IT, der Karl-Franzens-Universität Graz.

1 *BMI*, Sicherheit 2016 – Kriminalitätsentwicklung in Österreich 31, http://www.google.at/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwj8pdrnr-DTAhUMbBoKHcATADQQFggsMAA&url=http%3A%2F%2Fwww.bmi.gv.at%2Fcms%2FBK%2Fpublikationen%2Fkrim_statistik%2F2016%2FWeb_Sicherheit_2016.pdf&usg=AFQjCNEDiNqkAwEFnZakxqWQtnIxYaQZXQ (abgefragt am 8. 5. 2017).

2 Siehe dazu die von der Statistik Austria publizierten Verurteilungszahlen insb zu den Computerdelikten §§ 118a, 119, 119a, 126a, 126b, 126c StGB auf www.statistik.at (abgefragt am 8. 5. 2017).

3 Siehe fünf generelle Thesen zu den aktuellen Herausforderungen im Bereich des Computerstrafrechts bei *Bergauer*, Das materielle Computerstrafrecht (2016) 597 ff.

chen zu äußern. Ich kann allerdings in der mir zur Verfügung stehenden Zeit nicht auf alle mir wichtigen Aspekte dieses Vortrags eingehen.

Zutreffend thematisierte *Reindl-Krauskopf* sowohl in ihrem Sachverhaltsbeispiel zum „Smart Home-Hacking" als auch in ihren Ausführungen zum „Medjacking" § 118a StGB. Zu dieser Bestimmung ist allerdings anzumerken, dass sie seit ihrer Einführung im Jahr 2002[4] lange Zeit umstritten war, in den Jahren 2008[5] und 2016[6] aus diesem Grund novelliert wurde, und schließlich wohl nach wie vor umstritten ist. Wirft man einen Blick in die gerichtlichen Kriminalstatistiken der Jahre 2002 bis 2015 fällt auf, dass es in 14 Jahren lediglich 8 Verurteilungen österreichweit gab,[7] obwohl allein im Jahr 2014 677 Fälle eines Widerrechtlichen Zugriffs auf ein Computersystem angezeigt wurden.[8] Jeder, der sich den Wortlaut dieses Tatbestands ansieht, kann sich leicht selbst ein Bild von der Komplexität dieser Bestimmung machen. In beiden Sachverhaltsbeispielen (Smart Home-Hacking und Medjacking) ist auffällig, dass keine Feststellungen zum jeweiligen computertechnischen *modus operandi* bezüglich der „Überwindung einer spezifischen Sicherheitsvorkehrung" getroffen wurden, sondern dieser Sachverhaltskomplex mit dem Begriff „knacken" pauschalisiert wurde. Nach dem allgemeinen Sprachgebrauch bedeutet „knacken" aber nicht nur etwas physisch aufzubrechen oder durch Einwirken auf die Daten- bzw Sachsubstanz „auszuschalten", wie es im Vortrag verortet wurde, sondern insb auch einen Sperrmechanismus zu überlisten (man denke an die Wendung „einen Code knacken"). In solchen Formen computerspezifischer Handlungsweise liegt nun aber gerade das Wesen der Computerkriminalität im Allgemeinen und die besondere Herausforderung der Subsumtion solcher Sachverhalte unter den objektiven Tatbestand des § 118a StGB im Besonderen. Es ist daher notwendig, sich mit Fragen bezüglich des Überwindens (in Abgrenzung zur Verletzung und Umgehung[9]) ebenso auseinanderzusetzen wie mit der Frage, wie geeignet und tauglich eine Sicherheitsvorkehrung zu sein hat und wo eine solche angebracht bzw implementiert sein muss, um dem konkreten Tatobjekt „Computersystem" zurechenbar zu sein (zB im Falle eines LAN).[10] Wie sieht es aus, wenn zwei Wege ins Zielsystem führen, aber nur einer davon – was der Täter weiß – gesichert ist? Man denke etwa an ein externes Booten des fremden Computersystems oder den schlichten Ausbau der Festplatte, um diese Speichermedien auszulesen, ohne auf einen im System implementierten Sicherheitsmechanismus stoßen zu müssen. Wie wäre die Tatbestandsmäßigkeit iSd § 118a StGB zu beurteilen, wenn der Täter das zutreffende Passwort gekannt hätte? Wie ist der Täter in einem solchen Fall an das Passwort gelangt und welcher Aufwand ist hierfür notwendig gewesen, um das für eine „Überwindung" verlangte Mindestmaß an krimineller Energie[11] auszuloten und im Einzelfall festzustellen.[12] Wird darüber hinaus ein Schadprogramm zur Erlangung eines Passworts eingesetzt

4 StRÄG 2002 BGBl I 2002/134.
5 StRÄG 2008 BGBl I 2007/109.
6 StRÄG 2015 BGBl I 2015/112.
7 Siehe dazu die von der Statistik Austria publizierten Verurteilungszahlen auf www.statistik.at (abgefragt am 8. 5. 2017) (diversionelle Erledigungen wurden in diesen Statistiken nicht berücksichtigt).
8 Siehe die parlamentarische Anfragebeantwortung der Innenministerin betreffend die „Internetkriminalität – Strafdelikte durch IT-Medium im Jahr 2014" (AB 3400 BlgNR 25. GP 1).
9 Ein Überwinden erfordert mE die Konfrontation des Täters mit der spezifischen Sicherheitsvorkehrung, etwa durch Ausarbeitung eines Überwindungsplans und die anschließende direkte Bezwingung der Sicherheitsvorkehrung und verlangt daher mehr als ein bloßes Umgehen siehe *Bergauer*, Computerstrafrecht 100 f.
10 Siehe dazu insb *Bergauer*, Computerstrafrecht 88 ff.
11 Siehe dazu ErläutRV 285 BlgNR 23. GP 7; *Reindl-Krauskopf* in *Höpfel/Ratz* (Hrsg), Wiener Kommentar zum Strafgesetzbuch – StGB[2] § 118a Rz 28 (Stand 1. 10. 2014, rdb.at); *Bergauer*, Computerstrafrecht 98 f.
12 Zu diesen Fragestellungen siehe *Bergauer*, Computerstrafrecht 88 ff.

(wie etwa ein brute force-Tool zur Errechnung eines Passworts durch Permutation vordefinierter Zeichensätze bzw keylogger- bzw sniffer-Programme zum Abfangen von Zugangsdaten am Zielsystem bzw Übertragungsweg[13]), wäre auch an das Vorbereitungsdelikt des § 126c StGB zu denken.

Schaut man sich die komplizierten Elemente der überschießenden Innentendenz des subjektiven Tatbestands des § 118a StGB an, so fällt auf, dass aktuell gegenüber der Vorfassung die „Absicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden" entfallen ist und daher auch für bestimmte Fälle die Strafbarkeit (noch weiter) zurückgenommen wurde. Man denke an unberechtigte Geldtransaktionen über online-banking-Systeme durch Eingabe „abgefischter" Passwörter oder an Bitcoin-Mining über (zweckentfremdete) Bot-Netze. In solchen Fällen kommt es dem Täter nämlich nicht darauf an, im Sinne der Absichtlichkeit des § 5 Abs 2 StGB, einem anderen durch die Verwendung des Computersystems einen „Nachteil" zuzufügen (siehe § 118a Abs 1 Z 2 StGB). Dem Täter kommt es idR wohl ausschließlich darauf an, sich oder einem anderen einen Vermögensvorteil zuzuwenden bzw sich oder einen anderen zu bereichern. Die Zufügung eines – wie auch immer gearteten – Nachteils für andere wird daher vom Täter nur in Kauf genommen (arg *„dolus eventualis"*), nicht aber anvisiert.[14] Daran ändert sich auch nichts, wenn er das Eintreten eines solchen Nachteils bei einer anderen Person für gewiss hält. Es sollte daher diskutiert werden, ob für die Verwirklichung des subjektiven Tatbestands bezüglich des erweiterten Vorsatzes tatsächlich an der stärksten Form der Vorsatzausprägung, nämlich der Absicht, festgehalten werden sollte bzw ob nicht der entsprechende Teil der Definition der überschießenden Innentendenzen der Stammfassung des § 118a StGB (idF BGBl I 2002/134), dh die „Absicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden", wieder Eingang in den subjektiven Tatbestand finden sollte. Wer bei solchen Bereicherungsfällen an den Betrügerischen Datenverarbeitungsmissbrauch (§ 148a StGB) denkt, wird wohl damit konfrontiert, dass § 148a StGB ebenfalls aus legistischer Sicht nicht unumstritten konzipiert ist und folglich auch ein „Sammelbecken für Rechtsfortbildungen" darstellt.[15] So muss man sich etwa – wie ein Großteil der Lehre sowie die Rsp[16] – sehr weit „hinauslehnen", um das bloße Auslösen eines Datenverarbeitungsvorgangs (zB die Eingabe eines widerrechtlich erlangten aber zutreffenden Passworts) bereits als eine „Beeinflussung des Ergebnisses einer automationsunterstützten Datenverarbeitung" zu erachten.[17] Tatsächlich ist es wohl äußerst fraglich, ob dieses Delikt überhaupt jene strafbedürftigen Sachverhaltskonstellationen erfasst bzw „erfassen darf", für die es eigentlich geschaffen wurde.

Wie im Ausgangssachverhalt des Smart Home-Beispiels ersichtlich, kann das Opfer aber auch stundenlang keine Kontrolle über das System ausüben. Aus diesem Grund wäre daran zu denken, dass der Täter die Zugangsdaten geändert hat und das Opfer daher die Änderung selbst nicht – zB über die Bedienkonsole – rückgängig machen kann. Für solche Fälle wäre jedenfalls auch § 126a StGB (Datenbeschädigung) in den Varianten der Datenveränderung sowie Datenunterdrückung einschlägig. Da ein Smart Home-System aber neben Softwarekomponenten auch

13 Zur Beschreibung dieser Schadprogramme siehe an unterschiedlichen Stellen *Bergauer*, Computerstrafrecht.

14 Vgl *Bergauer*, Fall 12 – Phishing for nothing, in *Hinterhofer/Schütz* (Hrsg), Fallbuch Straf- und Strafprozessrecht[2] (2016) 189.

15 Siehe OGH 1. 6. 2006, 12 Os 45/06v (12 Os 46/06s); OGH 13. 10. 2005, 15 Os 99/05 f; siehe auch OLG Innsbruck 16. 12. 2014, 11 Bs 353/14w iZm Paysafecards; OGH 14.12.1995, 15 Os 131/95; *Bergauer*, Computerstrafrecht 353 ff mwN; *Bergauer*, Computerstrafrecht, in *Kert/Kodek* (Hrsg), Das große Handbuch Wirtschaftsstrafrecht (2016) Rz 11.136 f; *Komenda/Madl* in *Triffterer/Rosbaud/Hinterhofer* (Hrsg), StGB – Salzburger Kommentar zum Strafgesetzbuch[36] (2016) § 148a Rz 39 ff; weiters *Birklbauer/Hilf/Tipold,* Strafrecht Besonderer Teil I[3] (2015) § 148a Rz 7 f mwN.

16 Siehe die Positionen zusammenfassend *Komenda/Madl* in *Triffterer/Rosbaud/Hinterhofer*, SbgK[36] § 148a Rz 68.

17 Siehe dazu *Bergauer*, Computerstrafrecht 361 ff.

aus Hardwareteilen besteht (Thermostate, Schließmechaniken usw), die laut Sachverhalt nicht mehr ordnungsgemäß funktionieren, ist darüber hinaus in echter Konkurrenz an die Sachbeschädigung durch Unbrauchbarmachen iSd § 125 StGB zu denken.

Geradezu im Vorbeigehen wurde im Vortrag die einzig gerichtliche Strafbestimmung des § 51 DSG 2000[18] im Zusammenhang mit der Nutzung ausspionierter personenbezogener Daten angesprochen. Zur Aussage, dass das Sammeln solcher personenbezogener Informationen noch nicht strafrechtlich relevant sei, ist allerdings anzumerken, dass im sog „iPhone-Fall“[19] hinsichtlich des bloßen Speicherns digitaler Bildaufnahmen von einer Frau, welche sich gerade auf der Toilette befand, die grundsätzliche Anwendbarkeit des § 51 DSG 2000 bejaht wurde. Man muss daher wohl davon ausgehen, dass das Ermitteln der personenbezogenen Informationen durch den Täter mittels Kamerafunktion seines Smartphones als Akt des widerrechtlichen Verschaffens und das daran in unmittelbarer zeitlicher Abfolge erfolgte Speichern dieser (nunmehr digitalisierten) Daten auf der Speicherkarte des iPhones als Tathandlung des „Selbst-Benützens“ beurteilt wurde. Schließt man sich dieser Auffassung an, wäre – anders als im Vortrag kommuniziert – auch das bloße Sammeln personenbezogener Daten von § 51 DSG 2000 erfasst.[20]

Höchst interessant erweisen sich die von *Reindl-Krauskopf* in ihrem Vortrag angestellten Überlegungen zur Anwendung des § 118a StGB auf Fälle des sog „Medjacking“, gerade auch, weil sie selbst hierbei eine gewisse „Irritation“ verortet, die mE jedenfalls aus rechtspolitischer Sicht näher zu untersuchen wäre. Schon allein aus Sachlichkeitsüberlegungen wäre zu hinterfragen, ob aktive Implantate bzw Prothesen (wie zB bionische Arme oder Beine, Herzschrittmacher, Insulinpumpen usw) tatsächlich mit einer Sicherheitsvorkehrung iSd § 118a StGB ausgestattet sein müssen, um dem Träger einen strafrechtlichen Schutz vor Angriffen auf diese Prothesen zu gewähren? Vorauszuschicken ist, dass man als Mensch schon grundsätzlich keine „Ritterrüstung“ tragen muss, um seinen Willen zum Ausdruck zu bringen, nicht in der körperlichen Integrität verletzt werden zu wollen. Der im Vortrag angesprochene Fall des Medjacking könnte zur Verdeutlichung dieser Überlegungen etwas variiert werden. Man denke dabei an eine Sachverhaltsvariante, die nicht zu einer Tötung des Opfers führt, sondern sich die Tathandlung lediglich an einer bionischen Armprothese oder anderer elektro-mechanischer oder mittels Mikrochip gesteuerter, medizinischer Hilfsmittel (wie zB ionischem Auge, Retina-Stimulator, Hörgerät, funktioneller Muskelreizung, Neuro-Stimulator, Blasenschrittmacher usw) auswirkt. Der Täter manipuliert dabei das aktive Implantat, das per Bluetooth justiert und (fern-)bedient werden kann, derart, dass sich etwa ein bionischer Arm lediglich ständig auf und ab bewegt. Versucht man nun die Strafbarkeit einer solchen „Manipulation des Körpers“ zu ermitteln, zeigt sich schnell, dass es *de lege lata* schwierig ist, ein für solche Manipulationen geeignetes Delikt zu finden. Die Intensität der Beeinträchtigung der körperlichen Integrität erreicht wohl nach hM nicht die geforderte Intensität einer Körperverletzung iSd § 83 Abs 1 StGB. Bloße Misshandlungen sind noch keine Verletzungen am Körper.[21] Doch auch ein vorsätzliches Misshandeln iSd § 83 Abs 2 StGB scheidet aus, da wohl die fahrlässig herbeigeführte Folge fehlt (eine Gesundheitsschädigung mit Krankheitswert könnte sich allenfalls

18 BGBl I 1999/165 idF BGBl I 2009/133.

19 LG Salzburg 29. 4. 2011, 49 Bl 17/11v; *Thiele*, LG Salzburg: Datenverwendung in Schädigungsabsicht durch Aufnahme mit iPhone beim Toilettenbesuch, jusIT 2011, 185.

20 Siehe zu § 51 DSG 2000 ausführlich *Bergauer*, Computerstrafrecht 117 ff.

21 Siehe ganz allgemein *Burgstaller/Fabrizy* in *Höpfel/Ratz* (Hrsg), Wiener Kommentar zum Strafgesetzbuch – StGB[2] § 83 Rz 6 f (Stand 1. 8. 2016, rdb.at).

aufgrund eines aus der dauerhaften Manipulation entstehenden seelischen Leidens ergeben). Auch die Heranziehung des Delikts der Nötigung gem § 105 StGB wäre problematisch und zumindest im Lichte der Rsp wohl nicht anwendbar, da bei dieser Art der computertechnischen Manipulation nicht auf die Willensbildung des Opfers eingewirkt wird (arg *„vis absoluta"*). Für den OGH kommt prinzipiell nur *vis compulsiva* als Tatmittel der Nötigung in Frage.[22] Aber auch der hier relevante Gewaltbegriff bezüglich des Einsatzes „physischer Kraft" könnte zu Anwendungsschwierigkeiten der Nötigung im Zusammenhang mit computertechnischen Handlungsweisen des Medjacking führen. Des Weiteren wird auch die Sachbeschädigung durch Unbrauchbarmachen iSd § 125 StGB ausscheiden müssen, da nach hM nicht leicht zu entfernende Prothesen oder Implantate dem Körper zugerechnet werden und diese keine selbstständigen Sachen mehr darstellen.[23] Für solche mE strafwürdigen und strafbedürftigen Fälle bleibt *de lege lata* offenbar tatsächlich nur der „Widerrechtliche Zugriff auf ein Computersystem" (§ 118a StGB) übrig, allerdings lediglich unter der Voraussetzung, dass eine spezifische Sicherheitsvorkehrung im „Computersystem" vorhanden ist und diese vom „Hacker" auch überwunden wurde. Hier gibt es mE jedenfalls einen Nachbesserungsbedarf in der Strafrechtsdogmatik.

Die „digitale Erpressung" mittels des Einsatzes sog „Ransomware"[24] ist wohl das derzeit praxisrelevanteste Phänomen der im Vortrag angesprochenen Fallbeispiele. Da hier eine spezielle Schadsoftware, sog „Malware",[25] zum Einsatz kommt, wäre jedenfalls für diesbezügliche Vorbereitungshandlungen an das Vorbereitungsdelikt des § 126c StGB (Missbrauch von Computerprogrammen und Zugangsdaten) zu denken, das selbst wiederum jede Menge Besonderheiten aufweist.[26] Dieses Vorbereitungsdelikt tritt allerdings aufgrund materieller Subsidiarität zurück, sobald eines der dort in § 126c Abs 1 StGB genannten Hauptdelikte zumindest versucht wurde.

Abschließend möchte ich noch ein Statement zum letztbesprochenen Fall hinsichtlich vollautonomer Smart Cars abgeben. Die Entwicklungen im Bereich des maschinellen Lernens sind mittlerweile soweit fortgeschritten, dass intelligente Systeme tatsächlich eigenständig Entscheidungen treffen können. Es handelt sich dabei um selbstlernende Algorithmen, wie sie etwa im Bereich der Gesichtserkennung oder bei Fahrerassistenzsystemen in der Automobilindustrie bereits eingesetzt werden. Ein solches intelligentes System wird mittels eingespielter Beispieldatensätze quasi „erzogen". Das heißt, es werden nicht einfach Beispieldaten im System abgespeichert, welche in weiterer Folge bezüglich vordefinierter, dh dem System bereits bekannter, Sachverhalte abgerufen werden, sondern das System „erkennt" durch Analyse der Beispielsdaten Muster und Gesetzmäßigkeiten und wendet diese auf neue Szenarien völlig autonom auf Grundlage dieses „Erfahrungswissens" an. Aus heutiger Sicht ist es dabei undenkbar, alle möglichen Systementscheidungen hinsichtlich aller möglichen Sachverhalte vorauszudenken.

Besondere strafrechtliche Herausforderungen treten dabei insb bei einem verursachten Schaden im Zusammenhang mit selbstlernenden Algorithmen und einer etwaigen Fahrlässigkeitsstrafbarkeit in Erscheinung. Diese beginnen bereits bei der Frage, wer – also Programmierer, Hersteller uÄ –

22 Siehe dazu *Schwaighofer* in *Höpfel/Ratz* (Hrsg), Wiener Kommentar zum Strafgesetzbuch – StGB² § 105 Rz 24 und 27 (Stand 1. 5. 2016, rdb.at).

23 Vgl *Burgstaller/Fabrizy* in *Höpfel/Ratz*, WK² § 83 Rz 4; in diesem Sinne auch *Bachner-Foregger* in *Höpfel/Ratz* (Hrsg), Wiener Kommentar zum Strafgesetzbuch – StGB² § 190 Rz 4 (Stand 1. 11. 2009, rdb.at).

24 Siehe dazu *Bergauer* in *Kert/Kodek* Rz 11.31.

25 Zusammengesetztes Kurzwort für *„malicious software"*.

26 Siehe dazu ausführlich jüngst *Bergauer*, Computerstrafrecht 317 ff.

nach dem Schuldprinzip überhaupt als Tatsubjekt für das konkrete objektiv sorgfaltswidrige Verhalten der Maschine, das konzeptionell nicht immer mit einem Programmfehler verbunden sein muss, in Frage kommt und ob dieser Person der eingetretene Erfolg überhaupt objektiv zugerechnet werden kann. Hauptsächlich wird dabei wohl die Nachweisbarkeit im Bereich der normativen Zurechnung problematisch sein, wie vor allem die objektive Vorhersehbarkeit des Erfolgs oder die Frage nach der Risikoerhöhung bei rechtmäßigem Alternativverhalten, wenn nämlich einerseits gar kein Programmierfehler im Herstellungsprozess vorgelegen hat, sondern der Erfolg durch eine selbstständige Entscheidung im Rahmen der autonomen Fortentwicklung des Systems eingetreten ist, und andererseits, es faktisch gar nicht möglich ist, alle System-Entscheidungen im Hinblick auf sämtliche zukünftigen Sachverhaltskonstellationen vorherzusehen. Es wäre allerdings auch daran zu denken, dass etwa dem Hersteller und/oder Fahrzeughalter eine Überwachungspflicht für die besondere Gefahrenquelle „Smart Car" auferlegt sein kann, weshalb der Überwachungsgarant dafür Sorge tragen muss, dass andere Rechtsgüter durch die von ihm zu überwachende Gefahrenquelle nicht geschädigt werden dürfen (zB Verkehrssicherungspflichten). Wird gegen eine solche Überwachungsverpflichtung verstoßen, kann dies ebenfalls eine Fahrlässigkeitshaftung für den Einzelnen auslösen, sofern – wie für den Bereich der strafbaren Handlungen gegen Leib und Leben zutreffend – ein entsprechendes Fahrlässigkeitsdelikt existiert.

Unabhängig davon kann dem Halter eines voll-autonomen Autos ebenso wie dem Lenker eines Kfz, das nur gewisse Fahrmanöver unter der Aufsicht des Lenkers mittels Fahrerassistenzsystemen (wie zB Parkpilot) ausführt, eine sog „Einlassungsfahrlässigkeit" vorgeworfen werden, wenn ein autonomes Smart Car bzw ein Assistenzdienst in Betrieb genommen wird, obwohl dieses/ dieser bereits in der Vergangenheit ein dem Lenker bekanntes „auffälliges (Fehl-)Verhalten" gezeigt hatte.

Die Computerkriminalität ist aktuell wohl eines der unterschätztesten Kriminalitätsfelder, obwohl sie bereits zu einem massiven gesellschaftlichen Problem geworden ist. Die im Hauptvortrag angerissenen Phänomene bilden lediglich eine kleine Auswahl an Erscheinungsformen der Computerkriminalität. Im Jahr 2016 gab es allein in Österreich 13.103 Anzeigen wegen Cybercrime-Delikten.[27] Dennoch ist sie noch nicht wirklich in der Rechtsprechung angekommen, was die zu Beginn meines Kommentars präsentierten Verurteilungszahlen belegen dürften. Faktische Probleme der Täterausforschung, strafprozessuale Schwierigkeiten diverser informationstechnischer Ermittlungsmaßnahmen aber insb auch konzeptionell verbesserungsfähige Computerdelikte sind mE die Gründe dafür.[28] Proportional zur rasanten informationstechnischen Fortentwicklung und deren gesellschaftlichen Durchdringung werden jedenfalls die strafwürdigen Cybercrime-Phänomene in allen Lebensbereichen zunehmen, was zwingend auch dazu führen wird, dass der Computerkriminalität im Allgemeinen sowie der Computerstrafrechtsdogmatik im Besonderen in den nächsten Jahren eine viel höhere Aufmerksamkeit in Theorie und Praxis gewidmet werden muss, als ihr heute noch eingeräumt wird.

---

[27] *BMI*, Sicherheit 2016 – Kriminalitätsentwicklung in Österreich 31, http://www.google.at/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwj8pdrnr-DTAhUMbBoKHcATADQQFggsMAA&url=http%3A%2F%2Fwww.bmi.gv.at%2Fcms%2FBK%2Fpublikationen%2Fkrim_statistik%2F2016%2FWeb_Sicherheit_2016.pdf&usg=AFQjCNEDiNqkAwEFnZakxqWQtnIxYaQZXQ (abgerufen am 8. 5. 2017).

[28] Siehe fünf generelle Thesen zu den aktuellen Herausforderungen im Bereich des Computerstrafrechts bei *Bergauer*, Computerstrafrecht 597 ff.

AUSTRIAN LAW JOURNAL

ISSN: 2409-6911

DOI: 10.25364/1.4:2017.2.8
www.austrian-law-journal.at

Der digitalisierte Steuerzahler

Gregor Kirchhof*, Universität Augsburg

***Kurztext**: Die nach dem österreichischen Vorbild beschlossene Modernisierung des Besteuerungsverfahrens in Deutschland verletzt solange das Grundgesetz, bis ein Ertragsteuerrecht in Kraft tritt, das gesetzeskonform und gleichheitsgerecht digital angewandt werden kann. Auch die steuerlichen Erhebungslasten fordern eine Vereinfachung des materiellen Rechts: Selbst wenn die Mitwirkungspflichten, die Lenkungswirkungen, auch die steuerstrafrechtlichen Vorgaben und datenrechtlichen Lasten isoliert betrachtet noch zumutbar wären, verletzt jedenfalls deren Kumulation das verfassungsrechtliche Maß. Schließlich wird der Kampf gegen „aggressive Steuerplanungen" internationaler Unternehmen nur erfolgreich sein, wenn das anzuwendende Steuerrecht grundlegend vereinfacht wird. Diese Reformforderungen werden durch die historischen Motive der Soll-Ertragsbesteuerung bestätigt: Steuerhinterziehungen sollten vermieden, die Privatsphäre der Steuerpflichtigen sollte geschont und jeder gleichheitsgerecht zur Steuer herangezogen werden. Das geltende Steuerrecht belastet zu Recht den tatsächlichen, den Ist-Ertrag. Die geltende unübersichtliche Konkretisierung dieses Ausgangspunktes durch Elemente der Soll-Ertragsbesteuerung ist aber in einer grundlegenden Vereinfachung des Steuerrechts zu rationalisieren und zum System zu machen.*

***Schlagworte:** Modernisierung des Besteuerungsverfahrens, Steuerstrafrecht, Datenschutz im Steuerrecht, BEPS, kumulative Belastung, Ist- und Soll-Ertragsteuer.*

I. Die digitalisierte Erhebung von Steuern

Jeder, der Ertragsteuern entrichtet, ist ein „digitalisierter Steuerzahler". Das gilt in besonderer Weise in Österreich, weil hier die Einkommensteuer bereits seit Jahren idR automatisiert erhoben wird.[1] Deutschland folgte nun (endlich) diesem Vorbild und hat zu Beginn des Jahres die Modernisierung des Besteuerungsverfahrens[2] und damit den Regelfall einer *„ausschließlich automationsgestützten Steuerfestsetzung"*[3] in Kraft gesetzt. Dieser Schritt ist zwar nicht alternativlos, erinnert aber in Zeiten der Digitalisierung an diese Kategorie. Steuerrecht ist Massenfallrecht.[4] Die sehr hohe Zahl der

* Prof. Dr. *Gregor Kirchhof*, LL. M. ist Inhaber des Lehrstuhls für Öffentliches Recht, Finanzrecht und Steuerrecht sowie Direktor des Instituts für Wirtschafts- und Steuerrecht der Universität Augsburg.

1 Siehe hierzu *Ehrke-Rabel*, Die Rechtskraft von Abgabenbescheiden, in *Holoubek/Lang* (Hrsg), Rechtskraft im Abgaben- und Verwaltungsverfahren (2017) iE.

2 Gesetz zur Modernisierung des Besteuerungsverfahrens vom 18. 7. 2016 BGBl I 2016, 1679.

3 Entwurf eines Gesetzes zur Modernisierung des Besteuerungsverfahrens vom 3. 2. 2016 BT-Drs 18/7457, 48 f.

4 BVerfG 1 BvL 12/07 BVerfGE 127, 224 Rz 74 (Betriebsausgabenabzugsverbot); BVerfG 2 BvL 1/07 BVerfGE 122, 210 Rz 60 f (Pendlerpauschale); BVerfG 2 BvL 2/99 BVerfGE 116, 164 Rz 75 (Tarifbegrenzung für gewerbliche Einkünfte); vgl BVerfG 2 BvR 301/98 BVerfGE 101, 297 Rz 37 (häusliches Arbeitszimmer); BFH III R 53/00 BStBl II 2003, 565 Rz 44 (Eigenheimzulage); BFH III B 88/13, BFH/NV 2014, 517 Rz 15 (Kindergeldberechtigung); BFH X R 34/04, BFH/NV 2007, 68 Rz 57 (Kreditvermittlungsgebühren); BFH VIII R 42/02, BFH/NV 2006, 498 Rz 11 (Gewerbesteuerzerlegung); *Lang* in *Tipke/Lang*, Steuerrecht[20] (2010) § 4 Rz 132; *Hey* in *Tipke/Lang*, Steuerrecht[22] (2015) § 3 Rz 147.

Fundstelle: *Kirchhof*, Der digitalisierte Steuerzahler, ALJ 2/2017, 125–134 (http://alj.uni-graz.at/index.php/alj/article/view/91).

Betroffenen wird als zentrales Problem der Steuergesetze beschrieben[5] – auch des Ertragsteuerrechts, auf das sich die folgenden Ausführungen exemplarisch konzentrieren. Jeder, der Erträge erzielt, ist betroffen. Vergleichbar mit dem Straßenverkehrsrecht oder dem Kaufrecht gibt es zahlreiche gleich gelagerte Fälle. Eine digitalisierte Erhebung der Steuer drängt sich angesichts dieser Parallelität, der möglichen erheblichen Entlastung der Steuerbetroffenen im Steuerverfahren und der Chance auf, die Gesetzmäßigkeit und Belastungsgleichheit im Steuerrecht[6] zu verbessern.

Das Gesetz des Deutschen Bundestages zur Modernisierung des Besteuerungsverfahrens verfolgt das berechtigte und anspruchsvolle Ziel, die Steuererhebung idR automatisiert durchzuführen. Anstelle eines Finanzbeamten soll regelmäßig ein Rechner arbeiten. Der Fiskus konzentriert sich auf besondere Fälle, die eine Risikoprüfung oder der Zufall bestimmen.[7] Die Entlastung der Finanzverwaltung ist beträchtlich. Die Reform hat den Idealfall vor Augen, dass der Steuerpflichtige die Steuerdaten in den Rechner eingibt und kurz danach den Steuerbescheid digital erhält.

Doch legt bereits der Blick auf die Steuerbetroffenen die erhebliche Schieflage des in Deutschland bereits in Kraft getretenen Gesetzes offen. Die Finanzverwaltung ist dem komplizierten Steuerrecht nicht mehr gewachsen. Doch der Gesetzgeber reduziert nicht die Last durch ein einfacheres Steuerrecht, sondern entlastet einseitig die Verwaltung und belässt die Hauptlast bei den Steuerbetroffenen. Dies widerspricht der Wertung der grundrechtlichen Freiheitsrechte, den Steuerpflichtigen nicht über Gebühr zu beanspruchen.[8] Diese Digitalisierung des Steuerzahlers verletzt in Deutschland derzeit aus weiteren Gründen das Grundgesetz.[9] Die Frage, ob das vergleichbare Verfahren in Österreich gegen dort geltendes höherrangiges Recht verstößt, wird hier nicht behandelt. Im Ergebnis soll aber ein allgemeines Modell skizziert werden, wie ein modernes, automatisch anwendbares und zugleich datenschützendes Steuerrecht gestaltet sein könnte.[10]

II. Der gegenwärtige Verfassungsbruch: digitalisiertes Besteuerungsverfahren

Die in Kraft gesetzte automatisierte Anwendung des deutschen Einkommensteuerrechts gelingt nur, wenn alle Steuerbelasteten – die Steuerpflichtigen, die Arbeitgeber[11] und Banken[12] – die

5 *Isensee*, Die typisierende Verwaltung (1976) 52; *Isensee*, Resilienz von Recht im Ausnahmefall, in *Lewinski* (Hrsg), Resilienz des Rechts (2016) 33 (40); *Seer*, Der Vollzug von Steuergesetzen unter den Bedingungen einer Massenverwaltung, DStJG 31 (2008) 7 (16 ff); *Schmidt*, Moderne Steuerungssysteme im Steuervollzug, DStJG 31 (2008) 37 (38 ff); siehe auch die Nachweise in FN 4.

6 Zu diesem zentralen Anliegen des Steuerrechts: BVerfG 2 BvR 323/10 DStR 2016, 1731 Rz 101 (Altersvorsorgeaufwendungen); BVerfG 1 BvR 2664/09 NVwZ-RR 2010, 457 Rz 46 (Zweitwohnungssteuer); BVerfG 2 BvL 17/02 BVerfGE 110, 94 Rz 63 (Spekulationssteuer); BVerfG 2 BvR 301/98 BVerfGE 101, 297 Rz 38 (häusliches Arbeitszimmer); BVerfG 2 BvL 77/92 BVerfGE 96, 1 Rz 25, 31 (Weihnachtsfreibetrag); BVerfG 2 BvR 1493/89, BVerfGE 84, 239 Rz 104, 106, 109 (Zinsbesteuerung).

7 Entwurf eines Gesetzes zur Modernisierung des Besteuerungsverfahrens vom 3. 2. 2016 BT-Drs 18/7457, 48 f; zuvor *Schmidt*, DStJG 31 (2008) 38 ff; *Seer*, DStJG 31 (2008) 19 ff; *Seer*, Selbstveranlagung – Wegfall des Amtsermittlungsgrundsatzes? in DWS-Symposium (2014, 2015) 7 (10 ff).

8 *G. Kirchhof,* Die Überforderung der Arbeitgeber durch den Lohnsteuerabzug, FR 2015, 773 ff.

9 Siehe sogleich unter Pkt II. und III.

10 Siehe zum Folgenden insgesamt *G. Kirchhof,* Rechtsetzung und Rechtsanwendung im steuerlichen Massenfallrecht, DStJG 40 (2017) iE; *G. Kirchhof*, Renaissance der Sollertragsbesteuerung? in *Schön/Röder* (Hrsg), Zukunftsfragen des deutschen Steuerrechts III (2017) iE.

11 Siehe hierzu *G. Kirchhof*, Die Erfüllungspflichten des Arbeitgebers im Lohnsteuerverfahren (2005) 25 ff, 92 ff; *Drüen*, Inanspruchnahme Dritter für den Steuervollzug, DStJG 31 (2008) 167 (172 ff); *Drüen*, Die Indienstnahme Privater für den Vollzug von Steuergesetzen (2012) 133 ff.

12 *Scheurle*, Die Vollziehbarkeit der Besteuerung von Einkommen aus Kapital, DStJG 30 (2007) 39 (40 ff); *Tappe*, Privatisierung der Steuerverwaltung, in *Schön/Röder* (Hrsg), Zukunftsfragen des Steuerrechts III (2017) iE.

notwendigen Steuerdaten computergerecht aufbereiten.[13] Doch überfordert die Eingabe aufgrund des komplizierten Steuerrechts[14] die Betroffenen in aller Regel.[15] Wer die für die Steuererklärung maßgeblichen Steuerfragen alleine am Rechner beantworten will, wird nicht alle maßgeblichen Steuerdaten korrekt eingeben. In der Dateneingabe liegt eine zentrale Fehlerquelle des digitalisierten Verfahrens. Die beschlossene Reform hat bewusst nur das Verfahren modernisiert, nicht aber das materielle Steuerrecht vereinfacht. Der Gesetzgeber verkennt in dieser Trennung, dass sich nicht jedes Gesetz automatisiert anwenden lässt. Nur hinreichend klare Regeln – wie Geschwindigkeitsbeschränkungen – können ohne Beamte verwirklicht werden. Mit der gemessenen Überschreitung steht die Rechtsfolge fest. Das Steuerrecht ist aber gegenwärtig zu kompliziert, um idR automatisiert angewandt werden zu können. Die digitalisierte Steuererhebung verlangt daher eine Vereinfachung des materiellen Steuerrechts.[16]

Die in Kraft getretene automatische Anwendung eines wegen der Kompliziertheit nicht automatisch anwendbaren Steuerrechts belastet im Ergebnis nach Wahrscheinlichkeit und Vermutung. Dann aber wird strukturell auf die Gesetzmäßigkeit der Besteuerung und auf die Gleichheit im gesetzlichen Belastungserfolg[17] verzichtet – und dies im Bereich der Eingriffsverwaltung.

Zudem wurde entgegen der üblichen Bezeichnung kein *„automatischer Vollzug"* und auch keine *„ausschließlich automationsgestützte Steuerfestsetzung"*,[18] sondern etwas anderes beschlossen: eine *rechnergeleitete Selbstveranlagung.* Der Begriff des Vollzugs beschreibt die Konkretisierung der Gesetze durch eine bewusste Entscheidung der Rechtsanwendung.[19] Der Computer aber entscheidet – anders als der Mensch – nicht, er rechnet. Der steuerliche Gesetzesvollzug ist jedoch nicht in diesem Sinne berechenbar. Der Steuerpflichtige unterbreitet bei der Eingabe seiner Steuerdaten einen Subsumtionsvorschlag, den der Rechner vielleicht in Teilen korrigiert, regelmäßig aber übernimmt. Aus dem Rechtsgespräch mit der Finanzverwaltung wird ein Selbstgespräch am Rechner. Am Ende prägt die Rechtsauffassung des Steuerpflichtigen den Steuerbescheid. Der Rechtsstaat aber verlangt, dass die Verwaltung die Gesetzeskonkretisierung verantwortet.[20]

Die technischen Möglichkeiten geben der Finanzverwaltung erhebliche Informationen über die Steuerpflichtigen. Insb der landesweite Abgleich mit parallelen Fällen – von bestimmten Unternehmen, Zahnärzten, Rechtsanwälten oder Angestellten – verdeutlicht steuerliche Regelfälle und Abweichungen vom Normalfall. Der Fiskus hat überlegenes Wissen. Dann aber sollte er nicht den

13 Siehe zur notwendigen Koordination: Entwurf eines Gesetzes zur Modernisierung des Besteuerungsverfahrens vom 3. 2. 2016 BT-Drs 18/7457, 50, 100 ff, 119; *Gläser/Schöllhorn*, Die wesentlichen Neuerungen in der AO nach dem Gesetz zur Modernisierung des Besteuerungsverfahrens, DStR 2016, 1577 (1578).

14 Deutlich *Tipke*, Die Steuerrechtsordnung, Band III[2] (2012) 1393 ff; *Lang* in *Tipke/Lang* (Hrsg), Steuerrecht[20] (2009) VII (Vorwort); *P. Kirchhof*, Der sanfte Verlust der Freiheit (2004) 1 ff, 129 ff; *Mellinghoff*, Erneuerung des Steuerrechts – Reformüberlegungen am Beispiel der Besteuerung von Einkommen und Vermögen, DStJG 37 (2014) 1 (3); *Drüen*, Prinzipien und konzeptionelle Leitlinien einer Einkommensteuerreform, DStJG 37 (2014) 9 (12 ff); *Hey* in *Tipke/Lang*, Steuerrecht[22] § 3 Rz 1 ff; *Hüttemann*, Steuerrechtsprechung und Steuerumgehung, DStR 2015, 1146 (1148 mwH); *Schön*, Steuerpolitik 2008 – Das Ende der Illusion? DStR-Beihefter zu Heft 17/2008, 10 (10 ff).

15 Mit Blick auf die beschlossene Modernisierung des Besteuerungsverfahrens *G. Kirchhof*, FR 2015, 773 ff.

16 *G. Kirchhof,* FR 2015, 773 ff.

17 BVerfG 2 BvR 323/10 DStR 2016, 1731 Rz 101 (Altersvorsorgeaufwendungen); BVerfG 1 BvR 2664/09 NVwZ-RR 2010, 457 Rz 46 (Zweitwohnungssteuer); BVerfG 2 BvL 17/02 BVerfGE 110, 94 Rz 63 (Spekulationssteuer); BVerfG 2 BvR 301/98 BVerfGE 101, 297 Rz 38 (häusliches Arbeitszimmer); BVerfG 2 BvL 77/92 BVerfGE 96, 1 Rz 25, 31 (Weihnachtsfreibetrag); BVerfG 2 BvR 1493/89 BVerfGE 84, 239 Rz 104, 106, 109 (Zinsbesteuerung).

18 Entwurf eines Gesetzes zur Modernisierung des Besteuerungsverfahrens vom 3. 2. 2016 BT-Drs 18/7457, 48 f.

19 Siehe hierzu in der Perspektive des Gesetzes *G. Kirchhof*, Die Allgemeinheit des Gesetzes (2009) 304 ff.

20 Siehe zur tatsächlichen und faktischen Selbstveranlagung *Seer*, Der Vollzug von Steuergesetzen unter den Bedingungen einer Massenverwaltung, in DWS-Symposium (2014, 2015) 7 (10 ff); *Seer*, DStJG 31 (2008) 7 (31 ff).

Steuerpflichtigen das überkomplizierte Steuerrecht[21] in einem zum Scheitern verurteilten Versuch anwenden lassen, um mit technischer Hilfe die Anwendung sodann wie ein Beckmesser zu korrigieren – und dies unter der Drohung des Steuerstrafrechts.[22]

Vielmehr spielt der Rechtsstaat nach seinem Selbstverständnis mit offenen Karten. Das Recht auf informationelle Selbstbestimmung, das rechtliche Gehör und auch der Gedanke einer Wissens- und Waffengleichheit fordern generell, den Steuerpflichtigen umfassend über die ihn betreffenden Daten zu informieren. Dann aber ist der Schritt zu der vom Fiskus vorausgefüllten Steuererklärung nicht mehr weit – und auch hier bietet Österreich ein positives Beispiel. Steuererklärungen, die *in Teilen* von der Finanzverwaltung ausgefüllt werden, kennen zahlreiche Länder – auch Deutschland. In vielen Staaten ist die Steuererklärung aber im Regelfall *vollständig* vorausgefüllt.[23] Auch die vorausgefüllten Daten sind vom Steuerpflichtigen zu prüfen.[24] Die Steuerpflichtigen können, wenn sich nichts geändert hat, die Erklärung dann aber mit einem einfachen Placet abgeben. In Schweden reicht hierfür eine Kurzmitteilung (SMS), in Dänemark gilt das Schweigen nach einem Zeitablauf als Abgabe der Erklärung.[25] Die Erfolgsquote ist in den meisten Ländern bemerkenswert. Zum Teil werden über 70 % der Erklärungen nicht mehr korrigiert.[26] Verschiedene europäische Staaten haben sich für die idR vollständig vorausgefüllte Steuererklärung entschieden – Deutschland jedoch nicht.[27]

Soweit das Steuergeheimnis und der Kontrollauftrag des Fiskus dies erlauben, sollten die vorausgefüllten Steuererklärungen durch die überlegenen Informationen der Finanzverwaltung präzisiert und dem Steuerpflichtigen die Daten in diesen Erklärungen offengelegt werden. Die Erfolgsquote der Erklärungen würde erheblich gesteigert. Die Quote ließe sich durch eine Vereinfachung des Steuerrechts weiter erhöhen. Die Rechner der Finanzverwaltung würden ihre beträchtlichen Fähigkeiten nicht nur wie jetzt zur Entlastung der Finanzverwaltung, sondern auch für den Steuerpflichtigen einsetzen. Der Fiskus würde auffällige Punkte in jeder Steuererklärung markieren, die die Steuerlast erhöhen, aber eben auch senken könnten. Der Steuerpflichtige wäre umfassend informiert und steuerlich unterstützt. Das elementare Bewusstsein, dass jeder gleichheitsgerecht zur Besteuerung herangezogen wird, würde gestärkt, die Akzeptanz für die Steuerlast wahrscheinlich deutlich verbessert. Fehler würden auch in ihren möglichen steuerstrafrechtlichen Folgen verhindert. Zwar wird es immer Ausnahmefälle geben. Das Ziel aber ist, das Einkommensteuerrecht so zu vereinfachen, dass es idR auf Grundlage einer vorausgefüllten Steuererklärung automatisch angewandt werden kann. Dieses Ziel liegt nicht so fern, wie man meinen könnte.

---

21 Siehe FN 14 mwN.

22 Siehe unter Kap IV.

23 So etwa in Spanien, Dänemark, Schweden und den Niederlanden; siehe hierzu *Deloitte*, Comparative study of the personal tax return process[3] (2015) 7.

24 *Eichhorn,* Zum „Berechtigungsmanagement" für die „vorausgefüllte Steuererklärung", DStR 2013, 2722 (2723); *Vinken*, Vollmachtsdatenbank und vorausgefüllte Steuererklärung, DStR 2012, 1205 (1207).

25 *Herrmann*, Steuererklärung per SMS, SZ Nr 168 v 23. 7. 2013, 18; *Rothbächer*, Vorausgefüllte Steuererklärung: Potential für ein Erfolgsmodell, Legal Tribune Online, 14. 12. 2010, http://www.lto.de/persistent/a_id/2128/ (abgefragt am 21. 7. 2017).

26 *Rothbächer*, Vorausgefüllte Steuererklärung: Potential für ein Erfolgsmodell, Legal Tribune Online, 14. 12. 2010, http://www.lto.de/persistent/a_id/2128/ (abgefragt am 21. 7. 2017); *Eichhorn*, DStR 2013, 2723.

27 *Deloitte*, Comparative study[3] 6 f, wenngleich weitere Staaten zu nennen wären und die Abgrenzung einer in Teilen von einer überwiegend und auch einer vollständig vorausgefüllten Steuererklärung nicht einfach ist; siehe insgesamt auch *Rothbächer*, Vorausgefüllte Steuererklärung: Potential für ein Erfolgsmodell, Legal Tribune Online, 14. 12. 2010, http://www.lto.de/persistent/a_id/2128/ (abgefragt am 21. 7. 2017).

III. Die geltende Mischung aus Ist- und Soll-Ertragsbesteuerung ist zum System zu machen

Das geltende Steuerrecht zeichnet einen Weg, der eine weitgehende digitalisierte Anwendung des Steuerrechts ermöglichen könnte: Der Gesetzgeber sollte bewusst mehr Elemente der Soll-Ertragsbesteuerung nutzen. Ausgangspunkt des geltenden Einkommensteuerrechts ist zu Recht der Ist-Ertrag.[28] Die Ist-Ertragsteuer wird aus dem Leistungsfähigkeitsprinzip hergeleitet. Die Steuer richtet sich nach der tatsächlichen Leistungsfähigkeit, belastet einen bestehenden, einen Ist-Ertrag, der möglichst genau ermittelt wird. Die Soll-Ertragsteuer legt demgegenüber einen erwarteten Ertrag zu Grunde. So wurden die Erträge und die Steuerlast zB eines landwirtschaftlichen Unternehmens durch die preußische Klassensteuer aus dem Jahr 1820 nach äußeren Kriterien bemessen: der Nutzart, der Größe, der Lage, der Anzahl der Mitarbeiter und der sichtbaren Kapitalausstattung.[29] Diese Sollbesteuerung folgte *drei Erwägungen*. Der Vollzug ging dem Fiskus und den Steuerbetroffenen leicht von der Hand. Die Belastung der Steuerbetroffenen durch das Verfahren war äußerst gering, weil lediglich Äußerlichkeiten ermittelt werden mussten. *Zweitens* wurden die Daten der Steuerpflichtigen geschont, weil keiner die Finanzsphäre – den landwirtschaftlichen Betrieb – betreten musste. Schließlich wurden – *drittens* – in einer Gleichheit im Typus Steuerhinterziehungen verhindert.[30]

Die Soll-Ertragsbesteuerung wird zu Recht kritisiert. Erwirtschaftet der Steuerpflichtige mehr als die erwarteten Einnahmen, zahlt er eine im Vergleich zu seiner Leistungsfähigkeit geringere Steuer. Unterschreitet sein Ertrag die Erwartung, muss er eine Steuerschuld begleichen, die seine Leistungsfähigkeit übertrifft und ihn daher überfordert. Die Besteuerung des tatsächlichen Ertrags ist heute im Einkommensteuerrecht eine Selbstverständlichkeit.[31] Das geltende Recht ist gleichwohl von vielen Elementen der Soll-Ertragsbesteuerung geprägt. Die schedulenartige Besteuerung der Land- und Forstwirtschaft und der Kapitalerträge ist eine von solchen Elementen geprägte Sonderbehandlung.[32] Die zahlreichen Steuerbefreiungen des § 3 dEStG wollen ebenfalls Sondersituationen gerecht werden. Über die Einkunftsarten hinaus weist das gesamte Steuerrecht Elemente der Soll-Ertragsbesteuerung auf, insb in Abzugsverboten und Abzugsbeschränkungen, in der Absetzung für Abnutzung, in Freibeträgen und Freigrenzen sowie in Pauschalen.[33]

---

28 *Tipke*, Die Steuerrechtsordnung I: Wissenschaftsorganisatorische, systematische und grundrechtlich-rechtsstaatliche Grundlagen[2] (2000) 497 f; *Tipke*, Die Steuerrechtsordnung II: Steuerrechtfertigungstheorie, Anwendung auf alle Steuerarten, sachgerechtes Steuersystem[2] (2003) 631 ff; *Hey* in *Herrmann/Heuer/Raupach*, EStG, Einleitung, Anm 18; BFH I R 20/15 BFHE 252, 44 Rz 38 mwN (Vorlage Zinsschranke); BVerfG 2 BvL 37/91 BVerfGE 93, 121 Rz 50, 56 ff (Vermögensteuer); vgl BVerfG 2 BvR 2194/99 BVerfGE 115, 97 Rz 28 (Einkommen- und Gewerbesteuer).

29 *Knöller*, Die Besteuerung von Sollertrag und Istertrag (2015) 225 ff mwN.

30 Insgesamt *Knöller*, Besteuerung 225 ff mwN.

31 Siehe FN 29 mwN.

32 Schedulenartige Einkunftsarten: Land- und Forstwirtschaft (Besteuerung nach Durchschnittssätzen, § 13a dEStG); Besteuerung der Kapitalerträge (§ 2 Abs 5b dEStG; Verlustverrechnungsbeschränkung, § 20 Abs 6 S 1 dEStG; Sparer-Pauschbetrag, § 20 Abs 9 dEStG); Tonnagebesteuerung bei Handelsschiffen im internationalen Verkehr (§ 5a Abs 1 dEStG); für die Kapitalertragsteuer: *G. Kirchhof* in *Herrmann/Heuer/Raupach*, EStG, Einleitung, Anm 271.

33 Allgemeine Erwerbssphäre – Elemente der Soll-Ertragsbesteuerung: ua Zinsschranke (§ 4h dEStG, § 8a dKStG), Abzugsverbote (zB § 4 Abs 5 dEStG), private Kfz-Nutzung (§ 4 Abs 5 Z 6 S 2 ff, § 6 Abs 1 Z 4 S 2 ff dEStG, § 9 Abs 1 S 3 Z 4 f dEStG), Investitionsrücklage (§ 6b dEStG), Übertragung stiller Reserven (§ 6c dEStG), AfA (§ 7 dEStG), Investitionsabzugsbetrag (§ 7g Abs 1 dEStG), Sonderabschreibung für kleinere und mittlere Betriebe (§ 7g Abs 5, 6 dEStG), Werbungskostenpauschalen, Verlustverrechnungs- (zB §§ 20 Abs 6, § 23 Abs 3 S 7 f dEStG) und Verlustabzugsbeschränkungen (§ 10d dEStG), Verluste bei beschränkter Haftung (§ 15a dEStG), Freibeträge und Freigrenzen (zB § 13 Abs 3 dEStG), private Veräußerungsgewinne (§ 23 dEStG), Anrechnung der GewSt (§ 35 dEStG). Lohnsteuer – Elemente der Soll-Ertragsbesteuerung: ua Werbungskostenpauschalen (§ 9a dEStG), Verpflegungs-

Jede Bewertung und auch die steuerlichen Annahmen, dass ein PKW sechs, ein mobiles Telefon fünf und ein Notebook drei Jahre genutzt wird,[34] stimmen mit der Realität nicht überein, nähern sich dieser lediglich an. Werden in der Privatsphäre Abzüge zugelassen, nutzt das Recht auch hier Annäherungen.[35] Schließlich mündet das Einkommensteuerrecht in zwei groben Typisierungen: im Steuertarif und in den Progressionsgrenzen. Es ist schon erstaunlich, dass das Steuerrecht versucht, die Bemessungsgrundlage mit großem Aufwand genau zu ermitteln, um dann im Ergebnis insoweit pauschal zu besteuern.

So stehen wir vor einer bemerkenswerten Ambivalenz. Das deutsche Ertragsteuerrecht entscheidet sich zu Recht für den Ausgangspunkt der Ist-Besteuerung. Diese Grundentscheidung wird aber durch zahlreiche Elemente der Soll-Besteuerung verwirklicht. Das Ergebnis ist ein kaum stringentes unübersichtliches Mischsystem. Diese Mischung ist zu rationalisieren und zum System zu machen. Der Ausgangspunkt ist und bleibt die Ist-Ertragsbesteuerung. Sodann werden noch mehr Tatbestände typisiert und pauschaliert. Dann könnte die in Kraft getretene rechnergeleitete Selbstveranlagung[36] gesetzeskonform und gleichheitsgerecht gelingen und der Schritt zu einer vollständig vorausgefüllten Steuererklärung wäre nahe. Zudem würde der digitalisierte Steuerzahler erheblich entlastet.

IV. Die kumulative Überbelastung des digitalisierten Steuerzahlers

Steuern wollen die öffentliche Hand finanzieren. Diesen im Grunde einfachen Auftrag nutzen die Steuergesetze für eine Kaskade an Lasten. Selbstredend muss jeder seine Steuerschuld begleichen. Die Finanzlast rückt aber im Steuerverfahren zuweilen in den Hintergrund, obwohl nur sie den Zweck der Steuern erfüllt, die öffentliche Hand zu finanzieren. Hinzu treten *Lenkungswirkungen*, wenn durch steuerliche Lasten oder Vergünstigungen Verhalten beeinflusst werden soll.[37] Deutlich schwerer wiegen die erheblichen *Mitwirkungspflichten*. Nahezu alle Geldströme, nahezu alle Veränderungen in der Finanzsphäre müssen benannt und auch in ihrer Entwicklung dokumentiert werden. Die Steuerrechtsordnung zwingt den Steuerpflichtigen jährlich, vierteljährlich oder sogar monatlich zu einer aufwändigen technischen Geschicklichkeitsübung.[38] Die Steuerpflichtigen werden überfordert.

---

pauschalen (§ 9 Abs 4a dEStG), Lohnsteuerpauschalierungen (bei Sachzuwendungen: § 37b dEStG, in besonderen Fällen: § 40 dEStG, für Teilzeitbeschäftige und geringfügig Beschäftigte: § 40a dEStG, bei bestimmten Zukunftssicherungsleistungen: § 40b dEStG), Lohnsteuerklassen einschließlich der Zahl der Kinderfreibeträge (§ 38b dEStG), Faktorverfahren anstelle der Steuerklassenkombination III/V (§ 39 f dEStG).

34 *Bundesministerium der Finanzen*, AfA-Tabelle für die allgemein verwendbaren Anlagegüter vom 15. 12. 2000, Pkt 4.2.1, 6.13.2.2 und 6.14.3.2.

35 Privatsphäre – Elemente der Soll-Ertragsbesteuerung: ua Sonderausgaben nach § 10 Abs 1 dEStG (zB Betreuungskosten, Z 5; Begrenzung der Berufsausbildungskosten für die Erstausbildung, Z 7; Schulgeld für private Schulen, Z 9), Unterhaltsleistungen (§ 10 Abs 1a Z 1 dEStG), Vermögensübertragung gegen wiederkehrende Versorgungsleistungen (§ 10 Abs 1a Z 2 dEStG), Spendenabzug (§ 10b dEStG), Sonderausgaben-Pauschalbetrag (§ 10c dEStG), sonstige Begünstigungen nach §§ 10e, 10f, 10g, 10h, 10i dEStG, zumutbare außergewöhnliche Belastungen (§ 33 Abs 3 dEStG); siehe insgesamt und zum Existenzminimum: *Mellinghoff*, Privataufwendungen, in FS P. Kirchhof (2013) § 174 Rz 16 ff.

36 Siehe unter Kap II.

37 *G. Kirchhof*, Die lenkende Abgabe, Die Verwaltung 2013, 349 ff.

38 Insgesamt *Seer*, Verständigungen im Steuerverfahren (1996) 1 ff, 179 ff, 225 ff; *Müller-Franken*, Maßvolles Verwalten (2004) insb 135 ff; *Birk*, Das Gebot des gleichmäßigen Steuervollzugs und dessen Sanktionierung, StuW 2004, 277 ff; *Drüen*, Die Zukunft des Steuerverfahrens, in *Schön/Beck* (Hrsg), Zukunftsfragen des Steuerrechts (2009) 1 (18 ff); *Drüen*, Kooperation im Besteuerungsverfahren, FR 2011, 101 ff; mit Blick auf die Inanspruchnahme Dritter *G. Kirchhof*, Erfüllungspflichten; *Drüen*, DStJG 31 (2008) 167 ff; *Drüen*, Indienstnahme (siehe FN 11).

Die Überbelastung liegt auch darin, dass bei jeder falschen Angabe, die sich zum Nachteil des Fiskus auswirkt, die *Strafbarkeit* droht. Der objektive Tatbestand der Steuerhinterziehung wird erfüllt, wenn ein Steuerpflichtiger dem Fiskus unrichtige oder unvollständige Angaben macht und dadurch einen ungerechtfertigten Steuervorteil erlangt.[39] Das Steuerrecht ist gegenwärtig so kompliziert,[40] dass kaum eine Steuererklärung in diesem Sinne richtig ist. Die objektiven Tatbestandsvoraussetzungen liegen daher häufig vor. Jedenfalls leben die Steuerpflichtigen in der ständigen Ungewissheit, ob sie eine Steuererklärung abgegeben haben, die den objektiven Tatbestand der Steuerhinterziehung erfüllt.[41] Der *subjektive Tatbestand* stellt ebenfalls schwierige Abgrenzungsfragen, wenn keine Absicht vorliegt, sondern nur ein sog bedingter Vorsatz (*dolus eventualis*), der Täter also den Erfolg zwar nicht will, aber für möglich hält und billigend in Kauf nimmt.[42] Die hier bestehenden allgemeinen Abgrenzungsschwierigkeiten sind anerkannt, verschärfen sich aber angesichts eines unübersichtlichen Steuerrechts und der dadurch bewirkten Unsicherheiten über die Steuerschuld und damit den deliktischen Erfolg.[43] Die erheblichen Unsicherheiten werden dadurch verstärkt, dass das Steuerermittlungsverfahren mit seinen Mitwirkungspflichten nicht strikt vom Steuerfahndungsverfahren mit seinem Aussageverweigerungsrecht getrennt wird.[44] Der *Nemo-tenetur*-Grundsatz könnte – gelinde gesagt – besser umgesetzt werden. Die zentrale Aufgabe des Strafrechts, die Grenze zur Strafbarkeit klar zu ziehen, erfüllt das Steuerstrafrecht nicht.

Schließlich betrifft das geltende Steuerrecht den *Datenschutz* in erheblicher Weise. Der Steuerpflichtige wird verpflichtet und gedrängt, seine gesamten Finanzdaten offenzulegen, in der Erwerbs- und der Privatsphäre. Der Fiskus weiß über das Geschäftsmodell, die Geschäftspartner, die Familie, die Konfession, die Größe der Wohnung, über die Arbeiten in und an der Wohnung und über vieles mehr Bescheid. Der Steuerstaat fragt in der Absetzbarkeit sog außergewöhnlicher Belastungen sogar nach Krankheiten, also nach Informationen, die den intimen Bereich der Betroffenen nicht verlassen sollten.[45] Würden diese Daten mit moderner Technik verarbeitet, könnten die Profile, die Amazon, Apple und Google von uns erstellen, im Vergleich zu den Bildern, die die Finanzverwaltung zeichnen könnte, als kubistische Gemälde erscheinen. Die grundrechtliche Vorgabe, die Daten der Steuerpflichtigen zu schonen, wird gegenwärtig stark vernachlässigt. Dabei hat sich die Frage nach dem steuerlichen Datenschutz in Zeiten der Digitalisierung und modernen Datenverarbeitung erheblich intensiviert. Steuerdaten dürfen von Verfassungs wegen nur erhoben werden, wenn das Steuergeheimnis gewährleistet ist.[46] Es stellt sich die Frage, wie sicher die digitalen Steuerdaten sind. Grundlegender ist zu erörtern, ob für die Finanzierung des

39 § 371 Abs 1 Z 1 dAO.

40 Siehe FN 14 mwN.

41 *Kuhlen*, Grundfragen der strafbaren Steuerhinterziehung (2012) 100.

42 *Kaeser,* Steuerstrafrechtliche Verantwortung im Unternehmen und selbstregulierende Tax Compliance, DStJG 38 (2015) 193 (206 ff mwN); siehe aber auch *Kuhlen*, Vorsatz und Irrtum im Steuerstrafrecht, DStJG 38 (2015) 117 ff.

43 Deutlich *Kaeser,* DStJG 38 (2015) 206 ff.

44 *Herrmann*, Doppelfunktion der Steuerfahndung als Steuerkriminalpolizei und Finanzbehörde, DStJG 38 (2015) 249 ff; *Salditt*, Bürger zwischen Steuerrecht und Strafverfolgung, DStJG 38 (2015) 277 ff; *Drüen,* Außenprüfung und Steuerstrafverfahren, DStJG 38 (2015) 219 ff.

45 Krankheitskosten sind ein Musterfall außergewöhnlicher Aufwendungen, die von § 33 dEStG erfasst werden (*Kanzler* in *Herrmann/Heuer/Raupach*, EStG, § 33 EStG, Anm 90). § 33b dEStG knüpft unmittelbar an Behinderungen an. Entsprechende Nachweise sind vom Steuerpflichtigen zu erbringen (§§ 64 f dEStDV).

46 BVerfG 2 BvR 1439/89 BVerfGE 84, 239 Rz 136 ff (Besteuerung von Kapitaleinkünften); *Di Fabio* in *Maunz/Dürig*, Grundgesetz, Art 2 Rz 178; *Rüsken* in *Klein* (Hrsg), AO[13] (2016) § 30 AO Rz 2; *Alber* in *Hübschmann/Hepp/Spitaler*, Abgabenordnung – Finanzgerichtsordnung § 30 AO Rz 8.

Staates diese Masse an Daten erhoben werden muss. Die Soll-Ertragsbesteuerung hatte sich demgegenüber bewusst dafür entschieden, die Finanzsphäre der Steuerbetroffenen zu schonen.[47]

Der Datenschutz und das Steuergeheimnis werden gegenwärtig im Kampf gegen „*aggressive Steuergestaltungen*" internationaler Unternehmen erheblich gefährdet. Multinationale Unternehmen wie Amazon, Apple, Google oder Starbucks haben die Unterschiede nationaler Steuerrechtsordnungen genutzt, um ihre Steuerlast erheblich zu mindern. Gegen dieses sog *„Base Erosion and Profit shifting"* (BEPS) erwägen die Europäische Union[48] und die OECD[49] verschiedene Maßnahmen.[50] Bereits beschlossen ist das Country-by-Country-Reporting,[51] das die steuerliche Kooperation zwischen den Staaten verbessern soll. Daten multinationaler Unternehmen mit einem Umsatz von über 750 Mio Euro werden anderen Ländern bereitgestellt, in denen die Unternehmen steuerlich tätig sind. Erfasst werden die Verteilung des Umsatzes, des Gewinns, der Steuerlast, die Anzahl der Arbeitnehmer, bestimmte Vermögenswerte und die Geschäftstätigkeit jeder einzelnen Konzerneinheit.[52] Das entsprechende internationale Abkommen haben gegenwärtig 64 Staaten geschlossen.[53] Eine aggressive Steuergestaltung mag ein Land in einem isolierten Blick auf die vorhandenen Daten nicht erkennen oder ein bevorteiltes Land nicht entdecken wollen. In der überstaatlichen Zusammenarbeit aber werden – so die Erwägung – die Gestaltungen offengelegt und dann wirksam bekämpft. Die Unternehmensdaten werden, wenn die Unternehmen entsprechend tätig sind, über die gesamte Welt verteilt – in Europa, von Kanada bis nach Australien, von Südafrika bis nach Norwegen, von Brasilien bis nach China und Russland. Die Länder verpflichten sich im Vertrag zur Vertraulichkeit und zu einer angemessen Verwendung der Daten.[54] Ob alle 64 Staaten das Steuergeheimnis in angemessener Weise wahren, ist allerdings die zentrale Fragen. Zudem ist fraglich, ob die eher äußeren Informationen überhaupt helfen, „aggressive Steuerplanungen" aufzudecken. Die Grundrechte scheinen das Country-by-Country-Reporting zu verbieten, setzen ihm jedenfalls enge Grenzen. Auch deshalb drängt die *zentrale grundrechtliche Vorfrage*, welche Daten der Staat nutzen darf und soll, um Steuern zu erheben.

47 Siehe unter Kap III.

48 *Europäische Kommission*, Vorschlag für eine Richtlinie des Rates mit Vorschriften zur Bekämpfung von Steuervermeidungspraktiken mit unmittelbaren Auswirkungen auf das Funktionieren des Binnenmarkts, COM (2016) 26 final, http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52016PC0026&from=EN (abgefragt am 21. 7. 2017); Richtlinie (EU) 2016/1164 des Rates vom 12. 7. 2016 mit Vorschriften zur Bekämpfung von Steuervermeidungspraktiken mit unmittelbaren Auswirkungen auf das Funktionieren des Binnenmarkts, ABl L 2016/193, 1. Die Richtlinie wurde in Deutschland bereits umgesetzt (BGBl I 2016, 3000); siehe hierzu *Blumenberg/Kring*, Erste Umsetzung von BEPS in nationales Recht, BB 2017, 151.

49 OECD, Addressing Base Erosion and Profit Shifting, 2013 http://www.oecd-ilibrary.org/taxation/addressing-base-erosion-and-profit-shifting_9789264192744-en; siehe ferner die Abschlussberichte unter http://www.oecd.org/tax/aligning-transfer-pricing-outcomes-with-value-creation-actions-8-10-2015-final-reports-9789264241244-en.htm (jeweils abgefragt am 21. 7. 2017).

50 Siehe hierzu *Schön*, „Ein großer blinder Fleck", Gespräch über die Folgen von BEPS, EY TAX & LAW 04/2015 http://www.tax.mpg.de/fileadmin/TAX/docs/TL/WS/EY_BEPS_2.pdf (abgefragt am 21. 7. 2017).

51 Die OECD initiierte dazu das Multilateral Competent Authority Agreement on the Exchange of Country-by-Country Reports vom 27. 1. 2016 (http://www.oecd.org/tax/automatic-exchange/about-automatic-exchange/cbc-mcaa.pdf (abgerufen am 21. 7. 2017), eine entsprechende Richtlinie (EU) 2016/881 des Rates vom 25. 5. 2016 ist am 3. 6. 2016 in Kraft getreten. Auf nationaler Ebene sucht das Gesetz vom 20. 12. 2016 (BGBl I 2016, 3000), die Vorgaben umzusetzen.

52 Diese Bestandteile wurden in den neuen § 138a Abs 2 dAO übernommen.

53 Das Multilateral Competent Authority Agreement on the Exchange of Country-by-Country Reports haben aktuell 64 Länder unterzeichnet https://www.oecd.org/tax/automatic-exchange/about-automatic-exchange/CbC-MCAA-Signatories.pdf (abgefragt am 21. 7. 2017).

54 Section 5 des Multilateral Competent Authority Agreement on the Exchange of Country-by-Country Reports (FN 55) trägt dementsprechend den Titel "Confidentiality, Data Safeguards and Appropriate Use".

Selbst wenn die hier benannten Mitwirkungspflichten, Lenkungswirkungen, steuerstrafrechtlichen Vorgaben und datenrechtlichen Lasten isoliert betrachtet noch zumutbar wären, verletzt die *Kumulation aller Lasten* das verfassungsrechtliche Maß.[55] Das Steuerrecht will die öffentliche Hand durch eine angemessen Teilhabe an der Finanzkraft der Steuerpflichtigen finanzieren. Dieser Auftrag rechtfertigt die Massenbelastung aller Steuerpflichtigen, diese Lastenkumulation in Breite und Tiefe nicht.

V. Modernes Steuerrecht

Die Steuerpflichtigen erwarten vom Steuerrecht gegenwärtig vor allem eines: Rechtssicherheit – im Verfahren und in der Steuerlast. Im nationalen Recht fordern insb die Verschärfung des Steuerstrafrechts und die beschlossene automatisierte Steuererhebung klarere Steuernormen.[56] Ein Strich des Gesetzesgebers – um das berühmte Zitat *Julius von Kirchmann*[57] abzuändern – und ganze Steuer- und Compliance-Abteilungen müssen neu gegründet werden. Aktuell sind auf internationaler Ebene deutsche Unternehmen an über 1.000 steuerlichen Streitbeilegungsverfahren mit offenem Ausgang beteiligt. Wenn im Schnitt in jedem Verfahren um einen zweistelligen Millionenbetrag gerungen wird, besteht eine Planungsunsicherheit in Höhe eines zweistelligen Milliardenbetrages.[58] Ein allgemeines Steuergesetz ist auf internationaler, aber auch auf nationaler Ebene ein nachhaltiges Konjunkturprogramm[59].

Gegen ein reines System der Soll-Ertragsbesteuerung spricht das Leistungsfähigkeitsprinzip. Die steuerliche Leistungsfähigkeit ist nach dem tatsächlichen Ertrag zu ermitteln und nicht grob nach äußeren Kriterien zu schätzen. Doch könnte die notwendige Vereinfachung des Steuerrechts gelingen, wenn der Ausgangspunkt der Ist-Ertragsbesteuerung vermehrt durch Elemente der Soll-Ertragsbesteuerung konkretisiert und dabei die bestehende Mischung zum System gemacht wird. Denn die drei historischen Gründe, auf Grund derer sich die Soll-Ertragsbesteuerung bis weit in das 19. Jahrhundert in Deutschland behauptete, sind heute hoch aktuell.[60] Die Soll-Ertragsteuer war – *erstens* – einfach anzuwenden, man hätte sie vollständig automatisiert erheben können.[61] *Zweitens* wurden die Daten der Steuerpflichtigen geschützt, weil der Fiskus nicht nachforschen musste – er schaute auf die äußeren Kriterien.[62] Das einfache Steuerrecht vermied *drittens* Steuerhinterziehungen.[63]

---

55 Siehe zum grundrechtlichen Problem der „kumulativen Belastung" und der „grundrechtlichen Breitenwirkung" *G. Kirchhof*, Erfüllungspflichten 135 ff, 195 ff; *G. Kirchhof*, Grundrechte und Wirklichkeit (2007) 27 ff; *G. Kirchhof*, Kumulative Belastung durch unterschiedliche staatliche Maßnahmen, NJW 2006, 732 ff; zusammenfassend hinsichtlich der kumulativen Belastung: *Hillgruber*, Grundrechtlicher Schutzbereich, Grundrechtsausgestaltung und Grundrechtseingriff, Handbuch des Staatsrechts IX^3 (2011) § 200 Rz 97 ff mwN.

56 Siehe unter Kap II. und IV.

57 *Von Kirchmann*, Die Wertlosigkeit der Jurisprudenz als Wissenschaft (1969) 25.

58 Siehe für die Anzahl der Fälle und für Richtwerte über die allerdings schwer zu schätzende wirtschaftliche Bedeutung der Verfahren *Greil/Rasch*, Dispute resolution procedures in international tax matters – Germany, in *International Fiscal Association* (Hrsg), Cahiers de droit fiscal international, 101 a (2016) 263 (274 f); *Rasch/Mank* in *Kroppen/Rasch* (Hrsg), Handbuch Internationale Verrechnungspreise (23. Lfg Nov 2016) OECD-Kap IV, Anm 7; *Flüchter*, Seminar C: Verständigungsverfahren und die Beilegung grenzüberschreitender Streitigkeiten, IStR (2012) 694 (700), nennt exemplarisch Streitwerte von rund 200 und 700 Mio Euro.

59 Deutlich *Seer*, Diskussion, DStJG 39 (2016) 88: *„Die beste Wirtschaftsförderung ist nach wie vor ein neutrales Steuerrecht."*

60 Siehe insgesamt unter Kap III.

61 Siehe zu diesem aktuellen Anliegen unter Kap II.

62 Siehe zum Anliegen des Datenschutzes unter Kap IV.

63 Siehe insgesamt zu den Gründen unter Kap III.

Die Entwicklung des internationalen Steuerrechts[64] stellt zudem gegenwärtig eine grundlegende Gleichheitsfrage, die zu Zeiten der Soll-Ertragsbesteuerung im Vordergrund stand. Der Gleichheitsgedanke sollte nicht die Bemessungsgrundlage millimetergenau erfassen – das ist bei einer Soll-Ertragsteuer nicht möglich.[65] Das Gleichmaß erreichte sein Ziel, wenn alle gesetzeskonform zur Besteuerung herangezogen wurden. Der Augsburger Kilianplan aus dem 17. Jahrhundert suchte dieses Gerechtigkeitsanliegen zu erfüllen: Er diente der gleichmäßigen Erhebung der Vermögensteuer. Der koloriert gedruckte große Stadtplan wies durch goldene Striche und Nummern auf den Straßen und Häusern den Steuereintreibern den Weg, damit kein Steuerpflichtiger beim sog Steuerumgang ausgelassen wird.[66] Dieses Anliegen ist wieder aktuell. Doch heute einen vergleichbaren Plan zu zeichnen, der alle nationalen und übernationalen Steuerpflichtigen erfasst, ist unmöglich.

Bemerkenswert ist, dass die Vorschläge, die im Kampf gegen „aggressive Steuerplanungen" für eine Vereinfachung der Besteuerung übernationaler Unternehmen unterbreitet werden, an die preußische Klassensteuer von 1820 erinnern – eine Soll-Ertragsteuer. Die Erträge sollten hiernach nach parallelen äußeren Kriterien ermittelt werden.[67] Würde der Ausgangspunkt der Ist-Ertragsbesteuerung in Elementen der Soll-Ertragsbesteuerung konkretisiert,[68] würde die Digitalisierung des Besteuerungsverfahrens[69] besser gelingen und das Steuerstrafrecht das verfassungsrechtliche Maß besser wahren, weil bei einem einfacheren Steuerrecht der Rechtsbruch klarer zu erkennen ist. Die Daten der Steuerpflichtigen würden nachhaltiger geschützt, wenn sie von vornherein in einem deutlich geringeren Maße erhoben werden müssten.[70] In der Vereinfachung des Steuerrechts und dem dann möglichen automatischen Vollzug liegt die große Chance für das nationale und auch das internationale Steuerrecht, alle Steuerpflichtigen zu entlasten und gleichmäßig zu besteuern.

64 Siehe unter Kap IV.

65 Siehe unter Kap III.

66 *Cramer-Fürtig*, Aus 650 Jahren. Ausgewählte Dokumente des Stadtarchivs Augsburg zur Geschichte der Reichsstadt Augsburg 1156–1806 (2006) 112, benannt nach *Wolfgang Kilian* (1581–1662), der den Plan im Jahre 1626 schuf; siehe für ein Abbild eines Teiles (Lektion XLIV): http://cms.steuerforum-augsburg.de/ (abgefragt am 21. 7. 2017).

67 Siehe hierzu Kap III. und zu den Vorschlägen zur Reform des internationalen Steuerrechts *Feld* auf dem 59. Berliner Steuergespräch zum Thema „EU- und OECD-Initiativen gegen steuerliche Gewinnverlagerungen" (siehe für die Dokumentation [im Erscheinen] http://www.berlinersteuergespraeche.de).

68 Siehe unter Kap III.

69 Siehe unter Kap II.

70 Siehe insgesamt unter Kap IV.

AUSTRIAN LAW JOURNAL

ISSN: 2409-6911

DOI: 10.25364/1.4:2017.2.11
www.austrian-law-journal.at

Digitalisierung und Selbstbestimmung

Christoph Bezemek[*], Universität Graz

***Kurztext**: Der vorliegende Beitrag skizziert das Zusammenspiel von Digitalisierung und individueller Selbstbestimmung, stellt die Frage, welche Herausforderungen dieses Zusammenspiel birgt und diskutiert, wie ihnen begegnet werden kann.*

***Schlagworte:** Digitalisierung, Selbstbestimmung, Filterblase, Echokammer, soziale Netzwerke.*

I. Digitalisierung oder: Rhythm and Blues

Digitalisierung ist konzeptionell für die ersten beiden Jahrzehnte des 21. Jahrhunderts in etwa das, was Rhythm and Blues in der zweiten Hälfte des 20. Jahrhunderts war: Ein Begriff, an den man mit einem intuitiv geformten Vorverständnis herangeht, ohne dass man ihn genau bestimmen kann, der aber, will man eben dieses Vorverständnis nicht vielfach frustrieren, deshalb ein Stück weit definitionsavers ist; ein Begriff also, dem man ein weites Verständnis zubilligen muss, um dem gerecht zu werden, was gemeinhin darunter verstanden wird; zumal ja auch die Substantivierung in ihrer aktiven Ausgestaltung impliziert, dass es sich bei dem Phänomen um einen laufenden Prozess handelt, dessen weitere Entwicklung prognostizierbar, aber keineswegs ausgemacht ist.[1]

Festgehalten werden kann damit nur, dass der vorliegende Betrachtungsgegenstand lose um die Auswirkungen des umfassenden Einsatzes von Informationstechnologien im jeweiligen Problemfeld gruppiert ist. Und dieses Problemfeld ist konkret in unserem Fall eben, so kann man grob zusammenfassen, die Kapazität des Individuums, seine Lebensführung innerhalb und zugleich fernab des Gesellschaftsverbandes nach eigenem Dafürhalten auszurichten.[2] Im Zentrum der folgenden Überlegungen stehen damit insgesamt die Implikationen dessen, was *Luciano Floridi* aus ethischer Perspektive so wirkmächtig als 4. Revolution beschrieben hat.[3]

* Univ.-Prof. Dr.iur. *Christoph Bezemek*, B.A., LL.M. (Yale) ist Universitätsprofessor am Institut für Öffentliches Recht und Politikwissenschaft der Karl-Franzens-Universität Graz.

1 Vgl zu den verschiedenen Definitionsansätzen nur die Übersicht bei *Hess*, Digitalisierung, in *Gronau/Becker/Sinz/Suhl/Leinmeister* (Hrsg), Enzyklopädie der Wirtschaftsinformatik: Online-Lexikon http://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/technologien-methoden/Informatik--Grundlagen/digitalisierung (abgefragt am 12. 6. 2017).

2 Vgl dazu aus grundrechtlicher Perspektive bereits *Bezemek*, Allgemeine Handlungsfreiheit im System der österreichischen Bundesverfassung, ALJ 2016, 109.

3 *Floridi*, The 4th Revolution: How the Infosphere is Reshaping Human Reality (2014).

Fundstelle: *Bezemek*, Digitalisierung und Selbstbestimmung, ALJ 2/2017, 135–139 (http://alj.uni-graz.at/index.php/alj/ article/view/92).

II. Das extendierende Moment

Dass das eine weite Fragestellung ist, die im gegebenen Zusammenhang kaum umfassend behandelt werden kann, ist klar. Ebenso klar erscheint jedenfalls auf einen ersten Blick, dass, soweit die Optionen individueller Selbstbestimmung angesprochen sind, Digitalisierung zunächst als extendierendes Moment zu begreifen ist; ein Umstand, der besonders plastisch in der Verschränkung eigentlicher und virtueller Realität über interaktive oder kollaborative Prozesse des Web 2.0 zu Tage tritt, denen entschieden positive Auswirkungen auf die Handlungsspielräume des Einzelnen zukommen: Das gilt für die im weiteren Sinn soziale, für die sexuelle, aber auch für die politische Selbstbestimmung des Individuums: Noch nie war es so einfach, soziale Beziehungen anzubahnen, aufrechtzuerhalten oder auch abzubrechen. Ebenso mag es für eine qualifizierte Vielzahl der Bevölkerung noch nie so einfach gewesen sein, sich sozialen Interaktionen weitgehend zu verschließen und etwa notwendige Konsumgüter oder Dienstleistungen ohne zwischenmenschlichen Kontakt zu beziehen. Die Realisierung sexueller Bedürfnisse schöpft aus einer bekanntermaßen tiefen Quelle, die von der ubiquitären Verfügbarkeit pornographischer Inhalte bis hin zu spezifischen Applikationen reicht, die allein (oder jedenfalls vordringlich) der kurzfristigen Anbahnung erotischer Intermezzi dienen sollen. Und was die politische Dimension anlangt, muss die Potenz der 4. Revolution, auch für die Länder, in denen sie – im engeren Sinn – zu keinem Umsturz geführt hat, kaum bewiesen werden; allzu offenkundig und allzu einschneidend sind die Effekte, die hier von den Partizipations- und Organisationsmöglichkeiten digitaler Instrumente ausgehen.[4]

Aus rechtlicher Perspektive, zumal aus der Perspektive einer freiheitlichen Ordnung, scheint die Inanspruchnahme der so skizzierten Möglichkeiten digital katalysierter selbstbestimmter Lebensführung damit begrüßenswert; mehr noch: sie scheint dem dieser Ordnung zugrunde liegenden Leitbild des Individuums, das in seiner, über seine und auch abseits seiner gesellschaftlichen Einbettung selbstbestimmter und eigenverantwortlicher Akteur ist, in hohem Maße entgegenzukommen.

Selbstredend sind die üblichen Vorbehalte anzubringen, was Daten- und Privatsphärenschutz bis hin zum vielzitierten Recht auf Vergessenwerden anlangt;[5] insoweit Selbstbestimmung – jedenfalls dem Grunde nach – auf normativer Ebene stets bedingt, die Voraussetzung dafür zu schaffen, das Individuum *selbst* bestimmen zu lassen, in welchem Ausmaß die eigene Lebensführung entäußert wird. Dieser ausgetretene Pfad soll hier jedoch nicht beschritten werden.

4 Vgl dazu aus dem unüberschaubaren sozialwissenschaftlichen Schrifttum etwa *Shah/Cho/Eveland/Kwak*, Information and Expression in a Digital Age: Modeling Internet Effects on Civic Participation, Communication Research 2005, 531; *Mossberger/Tolbert/McNeal*, Digital Citizenship: The Internet, Society, and Participation (2008); *Gil de Zúñiga/Veenstra/Vraga/Shah*, Digital Democracy: Reimagining Pathways to Political Participation, Journal of Information Technology & Politics 2010, 36, oder die Texte bei *Allen/Light* (Hrsg), From Voice to Influence: Understanding Citizenship in a Digital Age (2015).

5 EuGH 13. 5. 2014, C-131/12, *Google Spain und Google*. Dazu nur aus dem neueren Schrifttum *Post*, Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere, Yale Law School, Public Law Research Paper 2017/598. Mit Blick auf Art 17 DSGVO vgl aus der aktuellen Handbuchliteratur den Abriss bei *Haidinger*, Die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch (Art 15–21 DSGVO), in *Knyrim* (Hrsg), Datenschutz-Grundverordnung: Praxishandbuch (2016) 125 (131–133).

Stattdessen ist eine andere Beobachtung in den Vordergrund zu rücken, die mit der genannten Herausforderung zwar nicht unbedingt verwandt, aber doch verschwägert ist und den zuvor geäußerten umfassend positiven Befund, was Digitalisierung und Selbstbestimmung anlangt, doch ein Stück weit relativiert.

Anzusetzen ist dabei freilich zunächst genau bei jenen Momenten, die das gegenständliche Phänomen in so hohem Maß positiv erscheinen lassen, was die Förderung selbstbestimmter Lebensführung anlangt: der ökonomisch und technisch niederschwellige Zugang zu endgeräteübergreifenden Anwendungen, die damit insgesamt das ermöglichen, was mittlerweile prominent unter dem Begriff des „*Onlife*" firmiert,[6] also eine Lebensführung, die zentral durch die Verwebung virtueller und realer Elemente gekennzeichnet ist; zugleich eine Lebensführung, die Rahmenbedingungen unterworfen ist, die sich in eben dieser Verwebung entwickeln; eine Lebensführung, die vielfach auf Basis der Nutzbarkeit der konventionellen Funktionen virtueller Teilhabe in den einzelnen Applikationen funktionale Konventionen etabliert, die sich in Erwartungshaltungen manifestieren und über diese zu sozialen Normen verdichten.

III. Jenseits des Limbus

Anders, und vielleicht ein wenig einfacher, formuliert: Aus dem Potenzial, bestimmte Formen sozialer Teilhabe in Anspruch zu nehmen, erwächst bei entsprechender Nutzungsfrequenz im realen sozialen Umfeld auch der Druck, diese Möglichkeit wahrzunehmen und sich damit nicht nur den expliziten Regeln der Nutzung, sondern auch den impliziten Usancen zu unterwerfen, die sich aus den Funktionalitäten der jeweiligen Applikation ergeben. Die Alternative dazu ist oftmals nur ein Leben im sozialen Limbus: Wer als Mittdreißiger keine Mitgliedschaft bei Facebook oder anderen sozialen Netzwerken vorweisen kann, wird wohl nur noch die Hälfte aller Einladungen zu den minderwichtigen Zusammenkünften seiner Freunde und Bekannten erhalten (wen dann unverhofft einmal eine Textnachricht mit der Bitte um eine Postanschrift erreicht, der weiß, dass eine Hochzeit ansteht). Wenn man jedoch einer jüngeren Generation angehört, erscheint die Teilnahme an virtuellen sozialen Netzwerken beinah alternativlos.[7]

Allzu viel Raum für Selbstbestimmung bleibt in diesem Zusammenhang nicht. Zugespitzt formuliert bedeutet es, sich mit beachtlicher Duldsamkeit formellen wie informellen Peer-review-Mechanismen (*Jon Ronson* hat dieses Phänomen treffend als *mutual grooming* bezeichnet)[8] zu unterwerfen, Feedbackschleifen, die vielfach dazu verhalten, die reale Lebensführung schon antizipativ mit ihrer virtuellen Repräsentanz in Einklang zu bringen; einer Repräsentanz, von der implizit klar ist, dass sie von einem bestimmten Erwartungsdruck der Umgebung geprägt ist, und die dementsprechend von der Dokumentation des soeben konsumierten Fünfgangmenüs über die Zurschaustellung intimer Aspekte der eigenen Körperlichkeit und die (oftmals auch als Konsequenz anzusehende) differenzierte Inanspruchnahme der Anzeige des Beziehungsstatus bis

6 Vgl wiederum *Floridi,* 4th Revolution 59–86.

7 Vgl nur das Datenmaterial bei *Perrin*, Social Networking Usage: 2005–2015, Pew Research Center (2015) http://www.pewinternet.org/files/2015/10/PI_2015-10-08_Social-Networking-Usage-2005-2015_FINAL.pdf (abgefragt am 12. 6. 2017). Aus entwicklungspsychologischer Perspektive vgl etwa *Antheunis/Schouten/Krahmer*, The Role of Social Networking Sites in Early Adolescents' Social Lives, Journal of Early Adolescence 2014, 1.

8 *Ronson*, So you've been Publicly Shamed (2015) 267.

hin zur photographischen Abbildung des eigenen Wahlverhaltens reicht.[9] *Max Webers* Vorstellung einer „*herrenlosen Sklaverei*"[10] bestellt Grüße...[11]

Indes wäre es naiv zu glauben, dass all das abseits virtueller Beziehungsgeflechte vernachlässigbar wäre. Auch reale soziale Netzwerke, wie könnte es anders sein, atmen eine vergleichbare Dynamik.[12] Und doch hat die digitale Umgebung unstreitig die Tendenz, diese Effekte zu verstärken, Konformität der Lebensführung zu befördern und durch die Homogenität des Lebenskreises Echokammern zu generieren, die über den Widerhall des Gleichen ähnliche Positionen validieren oder verfestigen.[13]

IV. Das hochgerechnete Leben

Die Eigengesetzlichkeiten, denen individuelle Entfaltung in einer digitalen Umgebung unterworfen ist, tun das Ihre, um diesen Befund zu ergänzen; innerhalb wie auch außerhalb virtueller sozialer Netzwerke. Besonders deutlich mag das in dem von *Eli Pariser* unter der Bezeichnung „Filterblasen" prominent gemachten Phänomen hervortreten:[14] Dass etwa idente Suchbegriffe in der Google-Maske unterschiedlicher Browser mit hoher Wahrscheinlichkeit unterschiedliche Ergebnisse zu Tage fördern, weil der leistungsfähige Algorithmus der Suchmaschine das so herangetragene Anliegen nicht im Vakuum, sondern vor dem Hintergrund der Präferenzen und Interessen, die er vergangenen Anfragen der Nutzerin oder des Nutzers entnimmt, verortet.[15]

Was auf einen ersten Blick im Verhältnis zum Vorhergesagten nicht als sonderlich konsequente Fortsetzung der zuvor umschriebenen Kritik erscheinen mag, ist es auf einen zweiten durchaus. Denn die Selbstbestimmtheit einer solcherart personalisierten Anfragebeantwortung kommt auch in dieser Betrachtung stets zum Preis eines gewissen Maßes an Selbstreferentialität. Ein wenig zynisch formuliert könnte man meinen: virtuell führen wir oftmals eben ein hochgerechnetes Leben.

Dass ebendas, gerade in der politischen Dimension, einen denkbar fruchtbaren Nährboden für die gegenwärtig so vielbeklagten postfaktischen Annahmen bietet, die die Debattenkultur negativ beeinflussen, ist alles andere als fernliegend. Echokammern und Filterblasen bieten frag-

9 Ein Verhalten, von dem der VfGH, 1. 7. 2016, W I 6/2016, Rz 536, annimmt, dass es „*keinen Verstoß gegen den Grundsatz der Freiheit der Wahl*" darstellt. Dem ist – so betrachtet – ohne Weiteres zuzustimmen. Fraglich (mE aber dem Grunde nach zu bejahen) ist indes, ob (und gegebenenfalls inwieweit) der Gesetzgeber iSd positiven Verpflichtungen, die aus dem Grundsatz des geheimen Wahlrechts erwachsen (vgl insb VfGH G 18/85 VfSlg 10.412) nicht gehalten ist, derartigen Praktiken entgegenzutreten, aus denen dem Individuum ohne Weiteres eine so offenkundige soziale Rechtfertigungslast erwachsen kann.

10 *Weber*, Wirtschaft und Gesellschaft[5] (1972) 709.

11 So bereits in diesem Zusammenhang *Zöllner*, Digitalisierung und Selbstbestimmung, tv diskurs 2016, 22 (23).

12 Womit keineswegs impliziert werden soll, dass reale und virtuelle soziale Netzwerke unverbunden neben einander stehen – vgl zu den vielfachen Schnittpunkten der beiden Sphären etwa die Darstellung bei *Boyd/Ellison*, Social Network Sites: Definition, History, and Scholarship, Journal of Computer-Mediated Communication 2007, 210 (221) mwN.

13 Dazu bereits *Bezemek*, Hate Speech, Shitstorm und Dschihad Online: Müssen die Grenzen der Meinungsfreiheit neu vermessen werden? in *Berka et al* (Hrsg), Meinungs- und Medienfreiheit in der digitalen Ära: Eine Neuvermessung der Kommunikationsfreiheit (2017) 43 (52–54) mwN.

14 *Pariser*, The Filter Bubble: What the Internet Is Hiding from You (2011).

15 Vgl nur die rezente Darstellung bei *Garcia-Rivadulla*, Personalization vs. privacy: An inevitable trade-off? IFLA Journal 2016, 227, sowie die Analysen von *Eisenberger*, Die Macht der Algorithmen: Der Verlust der Öffentlichkeit durch Personalisierung im Netz, juridikum 2011, 517 und *Mayrhofer*, Google, Facebook & Co: Die Macht der Algorithmen aus grundrechtlicher Perspektive, in *Berka et al* (Hrsg), Meinungs- und Medienfreiheit in der digitalen Ära: Eine Neuvermessung der Kommunikationsfreiheit (2017).

würdige Marktplätze diskursiver Auseinandersetzung; auch und insbesondere in epistemischer Perspektive.[16]

V. Sensibilität und Selbstverantwortung

Und doch scheint umfassende Larmoyanz nicht ohne Weiteres angezeigt. Denn jedenfalls der zugegebenermaßen banale Punkt, dass aus dem Blickwinkel individueller Selbstbestimmung die Chancen der Digitalisierung groß sind, ebenso aber auch ihre Herausforderungen, kann kaum in Abrede gestellt werden. Fraglich mag schon eher scheinen, wie die Chancen genutzt und die Herausforderungen bewältigt werden können. Tel quel dem für viele der hier nur angedeuteten Problemstellungen laut gewordenen Ruf nach verstärkter Regulierung nachzugeben, scheint oftmals die Realisierung der Chancen zugunsten der Vermeidung der Risiken zu opfern. Damit würde man sich nicht zuletzt der Möglichkeit begeben, Selbstbestimmtheit im virtuellen Umfeld über Selbstverantwortung zu generieren, Sensibilität zu entwickeln und Mündigkeit nicht nur als bloßes Lippenbekenntnis einzufordern.

Luciano Floridi mag recht haben, wenn er argumentiert, dass die 4. Revolution neue ethische Bewältigungsmuster braucht.[17] Ob das ebenso für rechtliche Instrumente gilt, mag jedenfalls mit guten Gründen bestritten werden.[18]

16 Dazu insb *Sunstein*, republic.com (2001). Zum Gesamtkomplex aus einer Meta-Perspektive auch *Sunstein*, Going to Extremes: How Like Minds Unite and Divide (2009).

17 *Floridi,* 4th Revolution.

18 Näher dazu *Bezemek*, Informationsblase und Grundrechte, in *ÖJK/Müller* (Hrsg), Krise der liberalen Demokratie? (in Druck).

AUSTRIAN LAW JOURNAL

ISSN: 2409-6911

DOI: 10.25364/1.4:2017.2.10
www.austrian-law-journal.at

Digitalisierung und Selbstbestimmung

Iris Eisenberger,* Universität für Bodenkultur Wien

***Kurztext**: Der Beitrag beleuchtet das Verhältnis von Digitalisierung und Recht. Am Beispiel der Blockchain-Technologie wird aufgezeigt, wie neue Formen und Räume der Selbstbestimmung geschaffen werden können. In distribuierten Systemen ist die Tendenz erkennbar, dass sich die rechtliche hin zu einer technologischen Steuerung verlagert. Wenn Funktionen, die für gewöhnlich der demokratisch legitimierte Gesetzgeber wahrnimmt, auf andere Systeme übergehen, führt dies zu Herausforderungen für rechtsstaatliche Demokratien. Fundamentale Fragen von Kontrolle und Machtbeschränkung iZm Digitalisierung stehen im Fokus. Der Beitrag plädiert schließlich für „legal foresight"-Forschung im Bereich neuer Technologien.*

***Schlagworte:** Blockchain-Technologie; distribuierte Systeme; dezentralisierte Systeme; zentralisierte Systeme; natürliche Person; juristische Person; elektronische Person; Verantwortung und Zurechnung; Demokratie.*

I. Einleitung[1]

Seit Jahrzehnten ist in den Rechtswissenschaften davon die Rede, dass durch Digitalisierung Selbstbestimmung verloren gehe.[2] Die Antithese, nämlich dass Digitalisierung neue Formen und Räume der Selbstbestimmung eröffnet, ließe sich ebenso begründet aufstellen. Die Frage, wie selbst- oder fremdbestimmt wir sind, adressiert das Kernproblem der Digitalisierung mE jedoch nicht. Digitalisierung führt dazu, dass Funktionen, die in rechtsstaatlichen Demokratien für gewöhnlich der demokratisch legitimierte Gesetzgeber und das Recht übernehmen,[3] zunehmend

* Univ.-Prof. Dr. Iris *Eisenberger*, MSc (LSE) ist Universitätsprofessorin und Leiterin des Instituts für Rechtswissenschaften der Universität für Bodenkultur Wien.

1 Für zahlreiche wertvolle Diskussionen danke ich Tina *Ehrke-Rabel*, Elisabeth *Hödl* und Konrad *Lachmayer*. Für die Unterstützung bei der Recherche und Ergänzung des Fußnotenapparats danke ich Franziska *Bereuter*, Sophie *Schmidt* und Lisa *Schranz*.

2 Siehe *Helbing et al*, Digitale Demokratie statt Datendiktatur, in *Könneker* (Hrsg), Unsere digitale Zukunft (2017) 3; *Spiecker,* Steuerung im Datenschutzrecht – Ein Recht auf Vergessen wider Vollzugsdefizite und Typisierung? Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaften 2014, 28; *Thiesse,* Die Wahrnehmung von RFID als Risiko für die informationelle Selbstbestimmung, in *Fleisch/Mattern* (Hrsg), Das Internet der Dinge (2005) 363.

3 Vgl *I. Eisenberger*, Zwischen Rechtswissenschaften und Life Sciences (in Druck); Zur Konfliktkanalisierungsfunktion des Rechts im Bereich von Risikotechnologien siehe *Stelzer*, Sicherheit durch Recht oder Rechtssicherheit? FORUM 1993, 56; Zur Steuerungsfunktion des Rechts siehe *Mayntz*, Soziale Dynamik und politische Steuerung: Theoretische und methodische Überlegungen (1997); Zur Funktion des Rechts als Ordnungs- und Friedenstifter siehe nur *Kelsen*, Reine Rechtslehre[2] (1960) 38 f.

Fundstelle: *Eisenberger*, Digitalisierung und Selbstbestimmung, ALJ 2/2017, 140–149 (http://alj.uni-graz.at/index.php/alj/ article/view/112).

durch andere Systeme wahrgenommen werden.[4] Die idR verfassungsrechtlich etablierte Kontrolle von Macht und die Vorbeugung von Machtmissbrauch[5] laufen damit zunehmend ins Leere.[6] Neue „Eliten", wie beispielsweise Software-EntwicklerInnen, etablieren mit ihren technologischen Innovationen gesellschaftliche Ordnungssysteme,[7] in denen sich regelmäßig die Werthaltungen der Programmierer widerspiegeln[8] und nicht die eines im demokratischen System errungenen gesellschaftlichen Konsenses. Dieser Beitrag zeichnet daher zunächst die Digitalisierung als eine recht(swissenschaft)liche Verlustgeschichte nach (II.), in weiterer Folge zeigt er anhand der Blockchain-Technologie, dass Digitalisierung auch neue Formen und Räume der Selbstbestimmung ermöglicht (III.), bevor er erörtert, ob digitalisierte, distribuierte Systeme von rechtlicher zu technologischer Steuerung führen (IV.) und vor welche Herausforderungen dieser Wandel demokratische Rechtssysteme stellt (V.) sowie schließlich, was daraus folgt (VI.).

II. Digitalisierung: Eine recht(swissenschaft)liche Verlustgeschichte der Selbstbestimmung

Die Frage, wie sich die Digitalisierung auf die Selbstbestimmung auswirkt, lässt sich leicht als recht(swissenschaft)liche Verlustgeschichte der Selbstbestimmung erzählen. Bereits Ende der 1960er Jahre steht im Mikrozensusbeschluss des deutschen Bundesverfassungsgerichts[9] zu lesen, dass es mit der Menschenwürde unvereinbar wäre, wenn der Staat Menschen zwangsweise gesamthaft registriert und katalogisiert und er sie in seiner Bestandsaufnahme wie Sachen behandelt;[10] daran würde auch eine anonym durchgeführte statistische Erhebung nichts ändern. Zugleich betonte das Bundesverfassungsgericht jedoch, dass *„[n]icht jede statistische Erhebung über Persönlichkeits- und Lebensdaten […] die menschliche Persönlichkeit in ihrer Würde [verletzt] oder […] ihr Selbstbestimmungsrecht im innersten Lebensbereich [berührt],"*[11] weshalb es die im Gesetz über die Durchführung einer Repräsentativstatistik der Bevölkerung und des Erwerbslebens (Mikrozensus) vom 16. 3. 1957[12] angeordnete Repräsentativbefragung zum Tatbestand „Urlaubs- und Erholungsreisen" als mit den Grundgesetz vereinbar erklärte.

4 Vgl *Ehrke-Rabel/I. Eisenberger/Hödl/Zechner*, Bitcoin-Miner als Prosumer: Eine Frage staatlicher Regulierung? Dargestellt am Beispiel des Glücksspielrechts, ALJ 2017 (in Endredaktion); *I. Eisenberger*, Innovation im Recht (2016) 152 ff; *Gruber/I. Eisenberger*, Wenn Fahrzeuge selbst lernen: Verkehrstechnische und rechtliche Herausforderungen durch Deep Learning? in *I. Eisenberger/Lachmayer/G. Eisenberger* (Hrsg), Autonomes Fahren und Recht (2017) 51; *Narayanan/Bonneau/Felten/Miller/Goldfeder*, Bitcoin and Cryptocurrency Technologies (2016) 282 f; *D. Tapscott/A. Tapscott*, Blockchain Revolution (2016) 271 ff.

5 Siehe *Adamovich/Funk/Holzinger/Frank*, Österreichisches Staatsrecht IV (2009) 10.

6 Siehe *I. Eisenberger*, Innovation 160.

7 Siehe *Ehrke-Rabel/I. Eisenberger/Hödl/Zechner*, ALJ 2017 (in Endredaktion); *Gruber/I. Eisenberger* in *I. Eisenberger/Lachmayer/G. Eisenberger* 51.

8 Siehe *Ehrke-Rabel/I. Eisenberger/Hödl/Zechner*, ALJ 3/2017 (in Endredaktion).

9 BVerfGE 27, 1 ff.

10 *„Es widerspricht der menschlichen Würde, den Menschen zum bloßen Objekt im Staat zu machen (vgl BVerfGE 5, 85 [204]; 7, 198 [205])"* BVerfGE 27, 1 (4). Demgegenüber werden „Maschinen" heute zunehmend wie Menschen behandelt; siehe *Beck,* Über Sinn und Unsinn von Statusfragen – zu Vor- und Nachteilen der Einführung einer elektronischen Person, in *Günther/Hilgendorf* (Hrsg), Roboter und Gesetzgebung (2013) 239; *Calo,* Robotics and the Lessons of Cyberlaw, Californian Law Review 2015, 513; *Hubbard,* "Do Androids Dream?" Personhood and Artificial Artefacts, Temple Law Review 2010, 405; *Kersten,* Relative Rechtssubjektivität – Über autonome Automaten und emergente Schwärme, Zeitschrift für Rechtssoziologie 2017, 8; *Müller-Hengstenberg/Kirn,* Intelligente (Software-)Agenten: Eine neue Herausforderung unseres Rechtssystems? MMR 2014, 307; *Schirmer,* Rechtsfähige Roboter? JZ 2016, 660; *Solum,* Legal Personhood for Artificial Intelligence, North Carolina Law Review 1992, 1231; *Teubner,* The Rights of Non-Humans: Electronic Agents and Animals as New Actors in Politics and Law, Journal of Law and Society 2006, 497.

11 BVerfGE 27, 1 (4).

12 dBGBl 1957/213.

Zählen, Registrieren und Katalogisieren beschäftigte die Gerichte immer wieder. Zentral ist dabei das Volkszählungsurteil des Bundesverfassungsgerichts. In seiner Entscheidung vom 15. 12. 1983[13] sprach das Gericht erstmals von einem Grundrecht auf informationelle Selbstbestimmung. Anlass dafür war das Volkszählungsgesetz 1983.[14] Über eine Volkszählung, Berufszählung, Wohnungszählung und Arbeitsstättenzählung sollten sämtliche EinwohnerInnen der Bundesrepublik Deutschland statistisch erfasst werden.[15] Nicht zuletzt die Furcht vor unkontrollierbarer Persönlichkeitserfassung führte zu den entscheidungsursächlichen Verfassungsbeschwerden.[16] Im Ergebnis entschied das Bundesverfassungsgericht, dass die *„[f]reie Entfaltung der Persönlichkeit […] unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus[setzt]. […] Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."*[17] Begründend führte das Bundesverfassungsgericht ua aus, dass technologische Innovationen die menschliche Persönlichkeit zunehmend gefährden, da sie es ermöglichen würden, vollständige Persönlichkeitsbilder zu erstellen und dies weitgehend unkontrollierbar durch die jeweils Betroffenen.[18]

Die Digitalisierung ermöglicht nicht nur, Personen umfassend zu zählen, zu registrieren und zu katalogisieren, sondern auch Personen und ihre Handlungen zu überwachen sowie die dabei eruierten Daten zu speichern und zu archivieren.[19] Überwachung dient dabei der Gewährleistung rechtskonformen Verhaltens einerseits und der Vorbeugung von Straftaten andererseits. Die zuvor erörterte, durch das deutsche Bundesverfassungsgericht konstatierte Gefährdung der freien Persönlichkeitsentfaltung und Selbstbestimmung trifft auf die vielfachen Überwachungsmöglichkeiten ebenfalls zu; auch diese haben die Gerichte in unterschiedlicher Weise beschäftigt.

Der österreichische VfGH prüfte beim Section-Control-Erkenntnis[20] das automatische Geschwindigkeitsmesssystem[21] auf seine Verfassungskonformität. Im Ergebnis hielt er die Datenermittlung und -verwendung zwar für zulässig, allerdings nicht flächendeckend und nur zweckgebunden, zur *„Überwachung der Einhaltung straßenpolizeilicher Vorschriften"*.[22] Diese Zweckbindung verpflichtet auch dazu, dass das Geschwindigkeitsmesssystem schon technologisch so gestaltet sein muss, dass unzulässig aufbewahrte Daten unverzüglich zu löschen sind.[23] Darüber hinaus ist die Überwachung auch vor Ort anzukündigen.[24] Ähnlich wie in den zuvor erörterten Entscheidungen des

13 BVerfGE 65, 1 ff.
14 Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung, dBGBl I 1982/369.
15 *„Mit der Volkszählung und Berufszählung werde ein vielfältiges Strukturbild der Bevölkerung in tiefer regionaler Gliederung gewonnen."* BVerfGE 65, 1 (11); siehe nur *Mendes,* Schutz vor Informationsrisiken und Gewährleistung einer gehaltvollen Zustimmung (2015) 24.
16 BVerfGE 65, 1 (3).
17 BVerfGE 65, 1 (31).
18 BVerfGE 65, 1 (30 f).
19 Für die Herausforderungen, die sich bei digitaler Überwachung im Namen von Anti-Terrormaßnahmen stellen siehe *Lachmayer/Witzleb*, The challenge to privacy from ever increasing state surveillance: a comparative perspective, UNSW Law Journal 2014, 748.
20 VfGH 15. 6. 2007, G 147/06 ua, 3.
21 § 100 Abs 5 b StVO 1960, BGBl 1960/159 idF BGBl I 2002/80 sowie des § 134 Abs 3 b Satz 1 Kraftfahrgesetz 1967, BGBl 1967/267 idF BGBl I 2002/80.
22 VfGH 15. 6. 2007, G 147/06 ua, 22.
23 VfGH 15. 6. 2007, G 147/06 ua, 22.
24 VfGH 15. 6. 2007, G 147/06 ua, 25. Mittlerweile haben die Sicherheitsbehörden gem § 54 Abs 6 Sicherheitspolizeigesetz, BGBl 1991/566 idF BGBl I 2017/130, die Möglichkeit, den öffentlichen Raum präventiv zu überwachen, dabei können sie Verkehrsdaten aus der Section Control verwenden.

Bundesverfassungsgerichts, lässt er die gegenständliche Datensammlung nur in eingeschränkter Weise zu. Auch wenn die Gefährdung der freien Persönlichkeitsentwicklung und der Selbstbestimmung vom VfGH nicht begründend herangezogen werden, ist naheliegend, dass die rechtsdogmatisch in erster Linie datenschutzrechtlich begründete Entscheidung auch dem Schutz der Selbstbestimmung gilt.[25]

Überwachen, Speichern und Archivieren spielen aber insbesondere bei der Aufklärung und Vorbeugung von Straftaten eine große Rolle und sie beschäftigten die Gerichte ebenfalls. Gegenstand höchstgerichtlicher und kontroversieller Entscheidungen waren dabei verschiedene Formen der Telekommunikationsüberwachung/Vorratsdatenspeicherung,[26] GPS-Überwachung,[27] Onlinedurchsuchung[28] oder automatisierte Kennzeichenerfassung.[29] Im Kern geht es bei all diesen Entscheidungen abermals um die grundrechtlich geschützte freie Persönlichkeitsentfaltung und Selbstbestimmung, die durch die Digitalisierung zunehmend gefährdet sind. Tenor der Entscheidungen ist, dass es einen unantastbaren Kernbereich höchstpersönlicher Lebensgestaltung gibt[30] und dass Befugnisse, die tief in das Privatleben hineinreichen und es ermöglichen, umfassende Persönlichkeitsprofile zu erstellen bzw verborgene Ermittlungsmethoden einsetzen, verfahrensrechtliche Vorkehrungen für einen effektiven Grundrechtsschutz benötigen.[31] Im Ergebnis dürfe auch die Kriminalitätsbekämpfung nicht dazu führen, dass Personen Erlebnisse höchstpersönlicher Art nicht mehr zum Ausdruck bringen können.[32]

Digitalisierung wird auch zum Sammeln von Daten genutzt, mit dem Ziel, diese miteinander zu verknüpfen und zu vergleichen. Dies geschieht beispielsweise bei der Rasterfahndung, bei der personenbezogene Daten miteinander abgeglichen werden, um jene Personen ermitteln zu können, welche für die Ermittlung relevante Merkmale aufweisen.[33] Das Bundesverfassungsgericht hält eine solche nur dann für zulässig, wenn eine konkrete Gefahr für hochrangige Rechtsgüter besteht, für eine Rasterfahndung im Vorfeld der Gefahrenabwehr bleibt jedenfalls kein Platz.[34]

Dieser Streifzug durch einschlägige Judikatur zeigt deutlich, dass der Verlust der Selbstbestimmung und der Schutz derselben seit den 1960er Jahren immer wieder Gegenstand höchstgerichtlicher Judikatur waren. Die zunehmende Digitalisierung und ihr staatlicher Einsatz lassen die Bereiche persönlicher Entfaltung und Selbstbestimmung enger werden. Neuere Entwicklungen, wie beispielsweise das Internet der Dinge, das Sensoren allgegenwärtig macht,[35] Big Data Analy-

25 Siehe idZ auch VfGH 27. 6. 2014, G 47/2012 ua.

26 BVerfGE 113, 348; BVerfGE 141, 220; VfGH 27. 6. 2014, G 47/2012 ua; EuGH 8. 4. 2014, C-293/12 ua, *Digital Rights Ireland und Seitlinger*.

27 BVerfG 12. 4. 2005, BVerfGE 112, 304 ff; U.S. Supreme Court 23. 1. 2012, 10-1259, *United States vs Jones.*

28 BVerfGE 120, 274 ff.

29 BVerfGE 120, 274 (378).

30 BVerfGE 113, 348 Rz 161; BVerfGE 112, 304 Rz 56.

31 BVerfGE 112, 304 Rz 61; BVerfGE 141, 220; EGMR 6. 12. 1978, 5029/71, *Klass vs Deutschland;* VfGH 27. 6. 2014, G 47/2012 ua.

32 BVerfGE 141, 220 Rz 121.

33 BVerfGE 115, 320 Rz 2.

34 BVerfGE 115, 320, Leitsatz 1.

35 Siehe nur *Christl*, Kommerzielle digitale Überwachung im Alltag, Studie im Auftrag der österreichischen Bundesarbeiterkammer (2014) 70; *Keller/Pütz/Siml*, Internet der Dinge, in *Mehler-Bichler/Steiger* (Hrsg), Trends in der IT 2012 (2012) 121; *Mattern/Flörkemeier*, Vom Internet der Computer zum Internet der Dinge, Informatik Spektrum 2010, 119; *Pohl,* Der bürgerliche Traum von digitaler Souveränität: Technische Bemerkungen zur völligen Unsicherheit digitaler Kommunikation, in *Friedrichsen/Bisa* (Hrsg), Digitale Souveränität, Vertrauen in der Netzwerkgesellschaft (2016) 11.

sen,[36] die die Vernetzung, Auswertung und Nutzung unterschiedlicher Daten quantitativ und qualitativ auf eine andere Ebene heben sowie algorithmische Entscheidungen in beinahe allen Lebensbereichen,[37] bringen zusätzliche Gefahren für eine Gesellschaft freier und selbstbestimmter Personen; eine Gesellschaft, die die Judikatur der letzten Jahrzehnte zumeist vergeblich versuchte zu schützen.[38] Neu an diesen Gefahren ist jedenfalls, dass sie vorerst kaum vom Staat selbst ausgehen,[39] sondern von Privaten. Private gefährden mit diesen Technologien die Privatsphäre anderer und manipulieren, diskriminieren und unterdrücken potenziell die technologienutzenden Personen.[40] Verknüpft man all diese Innovationen, lassen sich auch potentielle Verhaltensmuster einzelner Personen und Personengruppen vorhersagen.[41] Es braucht nicht allzu viel Phantasie, um zu erkennen, dass diese Entwicklungen den Raum für freie Persönlichkeitsentfaltung und Selbstbestimmung zusätzlich enger werden lassen.[42] Noch kleiner werden sie, wenn sich nicht ausschließlich Private, sondern zunehmend auch der Staat dieser Technologien bedient.

III. Blockchain-Technologien: Neue Formen und Räume der Selbstbestimmung

Die Geschichte der Digitalisierung und Selbstbestimmung ließe sich auch anders erzählen, nicht wie zuvor als Verlustgeschichte, sondern als eine, die neue Formen und Räume der Selbstbestimmung ermöglicht. Die, der Kryptowährung Bitcoin zugrunde liegende, Blockchain-Technologie verspricht beispielsweise in ihrer Geburtsstunde ein Mehr an Selbstbestimmung.[43]

Die Blockchain-Technologie lässt sich für viele unterschiedliche Anwendungen instrumentalisieren. Verschiedene Informationen lassen sich damit speichern und verwalten, beispielsweise

36 Siehe nur *Martini,* Big Data als Herausforderung für den Persönlichkeitsschutz und das Datenschutzrecht, DVBl 2014, 1481; *Weichert,* Big Data, Gesundheit und der Datenschutz, DuD 2014, 831.

37 Siehe nur *Finn,* What Algorithms Want: Imagination in the Age of Computing (2017); *Hofstetter,* Wenn intelligente Maschinen die digitale Gesellschaft steuern, in *Könneker* (Hrsg), Unsere Digitale Zukunft (2017) 37; *Lessig,* Code: Version 2.0, Basic Books (2006) 200 ff; *Nyholm/Smids,* The Ethics of Accident-Algorithms for Self-Driving Cars: an Applied Trolley Problem?, Ethical Theory and Moral Practice 2016, 1275; *Reichwald/Pfisterer,* Autonomie und Intelligenz im Internet der Dinge: Möglichkeiten und Grenzen autonomer Handlungen, CR 2016, 209; *Skistims/Voigtmann/David/Roßnagel,* Datenschutzgerechte Gestaltung von kontextvorhersagenden Algorithmen, DuD 2012, 31.

38 Sobald es neue Technologien gibt, werden sie auch eingesetzt und die bestehenden rechtlichen Schutzmaßnahmen erweisen sich regelmäßig als unzulängliche Schutzinstrumentarien. Kritisch dazu *Spiecker,* Zur Zukunft systemischer Digitalisierung – Erste Gedanken zur Haftungs- und Verantwortungszuschreibung bei informationstechnischen Systemen. Warum für die systemische Haftung ein neues Modell erforderlich ist, CR 2016, 699; *Cockfield,* Towards a Law and Technology Theory, Manitoba Law Journal 2004, 383 (405); ferner *Reidenberg*, Lex Informatica: The Formulation of Information Policy Rules through Technology, Texas Law Review 1998, 554.

39 Freilich werden neue Technologien auch von Staaten eingesetzt und gefährden eine Gesellschaft freier BürgerInnen. Siehe dazu stellvertretend für Vieles die Diskussion um den Einsatz unbemannter Drohnen. *Schöberl,* „Global Battlefield?" Drohnen und der geographische Anwendungsbereich des humanitären Völkerrechts, in *Gramm/Weingärtner* (Hrsg), Moderne Waffentechnologie (2015) 120–131; *Mützenich/Bieger,* Wege des völkerrechtlichen Umgangs mit Kampfdrohnen, S&F 2014, 25; *Löffelmann,* Der Einsatz von Kampfdrohnen zur Terrorismusbekämpfung im Schnittpunkt von humanitärem Völkerrecht und Menschenrechtsstandards, KJ 2013, 372; *Zimmermann,* Völkerrechtliche Fragen des Einsatzes bewaffneter Drohnen, MRM 2013, 96.

40 Siehe *Weichert*, Big Data und Datenschutz, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, 1.

41 Siehe *Martini,* Big Data als Herausforderung für den Persönlichkeitsschutz und das Datenschutzrecht, DVBl 2014, 1481.

42 Siehe idZ auch *Martini,* DVBl 2014, 1481.

43 Vgl *Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System (2008), https://bitcoin.org/bitcoin.pdf (zuletzt abgefragt am 13. 11. 2017).

Transaktionen, Verträge oder Rechte.[44] Die Blockchain ist eine, unzählige Male replizierte, digitale Datenbank, in der alle Transaktionen eines bestimmten Netzwerkes gespeichert werden. Die Netzwerkteilnehmenden sind miteinander verbunden, in einem sog Peer-to-Peer-Netzwerk. Die jeweiligen Transaktionen werden dabei vereinfacht gesagt, wie einzelne Glieder in einer Kette aneinandergereiht. Die getätigten Transaktionen werden auf jedem Knoten, der Teil des Netzwerkes ist, eins zu eins abgebildet. Die Daten werden demnach nicht zentral gespeichert und verwaltet, sondern verteilt auf alle Netzwerkteilnehmenden.[45]

Weil die Blockchain auf allen teilnehmenden Knoten abgespeichert wird, gilt sie als besonders sichere Technologie, da Änderungen bei allen TeilnehmerInnen zugleich erfolgen müssen.[46] Um die Identität und die Daten der Netzwerkteilnehmenden zu schützen, sind sie pseudonymisiert.[47] Die der Blockchain zugrunde liegende Software ist Open Source, also für alle transparent und gleichermaßen zugänglich.[48]

Die meisten webbasierten Software-Applikationen arbeiten auf der Grundlage eines zentral organisierten Server/Client-Modells. Dabei wird der Informationsfluss von einer zentralen Stelle aus verwaltet und kontrolliert. Die bekanntesten NutzerInnen dieses Modells sind beispielsweise Facebook, Google und Amazon. Dezentralisierte Systeme sind hingegen Systeme, in denen der Informationsfluss nicht von einer zentralen Stelle aus verwaltet wird, sondern von einigen, wenigen Knotenpunkten. Distribuierte Systeme sind demgegenüber Systeme, bei denen der Informationsfluss von allen Teilnehmenden zugleich verwaltet und kontrolliert wird.[49]

Eine der Besonderheiten der Blockchain-Technologie ist, dass sie keine zentral verwaltete Datenbank ist, sondern als distribuierte Datenbank angedacht ist.[50] Dies trifft jedenfalls auf die Konsensbildung bei der Kryptowährung Bitcoin zu, zu der alle System-TeilnehmerInnen gleichermaßen beitragen können.[51] Das Bitcoin-Mining ist ebenfalls distribuiert konzipiert und wäre theoretisch allen NetzwerkteilnehmerInnen möglich; aufgrund der hohen Kosten, die mit dem Bitcoin-Mining verbunden sind, lassen sich in der Praxis Tendenzen hin zu einem dezentralisierten System beobachten.[52] Der Code selbst kann hingegen als ein zentralisiertes Element des Systems betrachtet werden.

44 Siehe nur *Ehrke-Rabel/I. Eisenberger/Hödl/Zechner*, ALJ 2017 (in Endredaktion).

45 Zur Blockchain-Technologie und den verschiedenen Anwendungsmöglichkeiten siehe *Ehrke-Rabel/I. Eisenberger/Hödl/Zechner*, ALJ 2017 (in Endredaktion); *Raval*, Dezentralized Applications (2016); *D. Tapscott/A. Tapscott*, Blockchain; *Narayanan/Bonneau/Felten/Miller/Goldfeder*, Bitcoin, mit jeweils weiteren Hinweisen.

46 Kritisch zur vermeintlichen Sicherheit siehe *Ehrke-Rabel/I. Eisenberger/Hödl/Zechner*, ALJ 2017 (in Endredaktion).

47 *Ehrke-Rabel/Hödl,* Effizienter Steuervollzug im Lichte des Datenschutzes, in *Jahnel* (Hrsg), Jahrbuch Datenschutzrecht (2016) 231 (253 f); *Diedrich*, Ethereum 126.

48 Die Software für Etherum ist etwa direkt auf der Homepage zugänglich: https://www.ethereum.org (zuletzt abgefragt am 13. 11. 2017).

49 Siehe idZ *Raval*, Dezentralized Applications 2 ff.

50 Vgl *Nakamoto*, Bitcoin.

51 Siehe *Narayanan/Bonneau/Felten/Miller/Goldfeder*, Bitcoin 28 f.

52 Siehe *Narayanan/Bonneau/Felten/Miller/Goldfeder*, Bitcoin 272 ff. (De)Zentralisierung entsteht beispielsweise auch durch Wallets und Börsen.

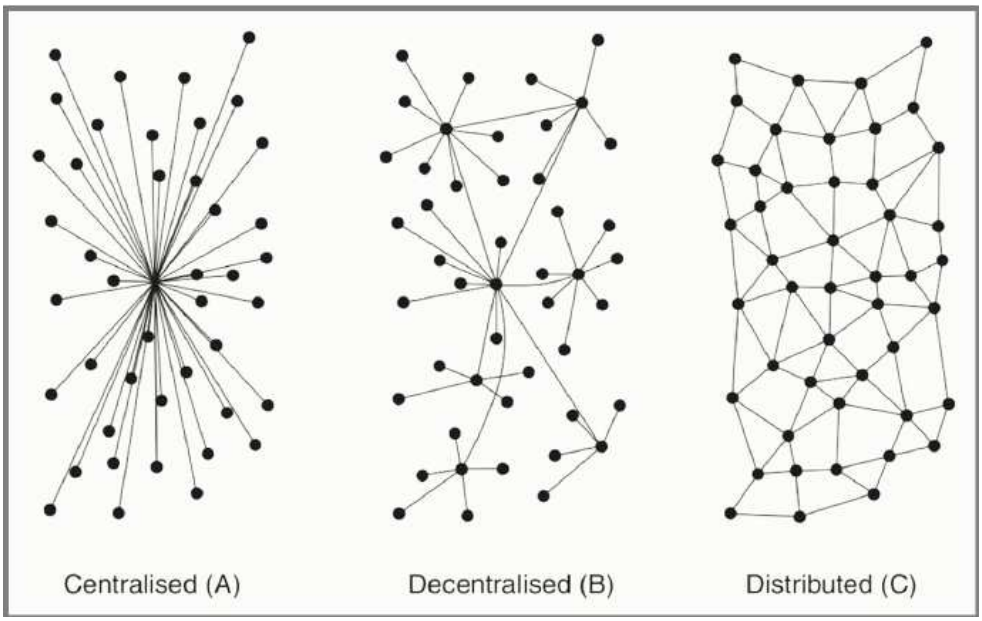

Abb 1: Centralised, decentralised and distributed network models[53]

Digitale Online-Datenbanken, an denen man nur verschlüsselt teilnehmen kann und die nicht zentral, sondern von allen Teilnehmenden verwaltet werden, bauen die Privatsphäre aus.[54] Aufgrund der Pseudonymisierung in der Blockchain sind die gesammelten Daten kaum rückverfolgbar,[55] ebenso schlecht lassen sich die Aktivitäten in einer privat aufgesetzten Blockchain aufgrund der mangelnden zentralisierten Verwaltung staatlich überwachen oder kontrollieren. All dies eröffnet neue Formen der Persönlichkeitsentfaltung und technologisch geschützte Räume der Selbstbestimmung. Anders als die zuvor erzählte Verlustgeschichte lässt sich die zunehmende Digitalisierung demzufolge auch als Geschichte eines Selbstbestimmungsgewinns erzählen.

Nicht übersehen werden darf in diesem Zusammenhang aber, dass Software das Verhalten seiner NutzerInnen normiert.[56] NutzerInnen können nur in den Grenzen des Codes agieren. Der Code lässt sich, im Unterschied zu rechtlichen Normen, nur mit Spezialwissen umgehen oder brechen. Der Code wirkt insofern ähnlich wie eine Bremsschwelle auf der Straße, sie zwingt die FahrerIn zu einem Bremsmanöver und verringert dadurch den persönlichen Handlungsspielraum. Der der Blockchain zugrunde liegende Code schafft in diesem Sinn nicht nur Räume der persönlichen Entfaltung und Selbstbestimmung, sondern engt diese auch ein, je nach Ziel des Systems in unterschiedlicher Intensität. Die Seratio Blockchain beispielsweise strebt die Messbarkeit immaterieller Werte an, etwa Liebe, Freundlichkeit, Freiheit oder Religion.[57] Werte wie diese, die unwiderrufbar und unlöschbar in einer Blockchain festgehalten werden, können die Freiheit und die Selbstbestimmung der NutzerInnen nachhaltig einschränken. Die Frage nach dem Verlust von oder dem Gewinn an Selbstbestimmung erscheint dann aber falsch gestellt. Die Frage

53 *Baran,* On distributed communications: I. Introduction to distributed communications network (1964) 2.
54 Siehe idZ *Narayanan/Bonneau/Felten/Miller/Goldfeder*, Bitcoin 168 ff.
55 Siehe *Ehrke-Rabel/Hödl* in *Jahnel* 231.
56 Grundlegend zur normativen Qualität technologischer Systeme siehe *Winner*, Do Artifacts Have Politics? in *Daedalus* (Hrsg), Modern Technology: Problem or Opportunity (1980), https://transitiontech.ca/pdf/Winner-Do-Artifacts-Have-Politics-1980.pdf (zuletzt abgefragt am 19. 7. 2017) 121.
57 Siehe http://www.the-blockchain.com/docs/Seratio%20Blockchain%20Whitepaper%20%2826%20October%202016%29%20%5bv1.2%5d.pdf (zuletzt abgefragt am 12. 11. 2017).

ist nicht mehr, ob wir fremd oder selbst bestimmt sind, sondern woher wir überhaupt wissen, wer bestimmt bzw wie wir diejenigen, die bestimmen, wieder sichtbar und verantwortlich machen.

IV. Digitalisierte distribuierte Systeme: Von rechtlicher zu technologischer Steuerung

Distribuierte Systeme, wie das auf der Blockchain-Technologie beruhende Bitcoin-Netzwerk, sind Systeme, in denen die teilnehmenden Personen idR nur dann rechtlich sichtbar und greifbar werden, wenn sie von der virtuellen in die reale Welt wechseln, etwa, wenn sie Bitcoin in Euro wechseln.[58] Die mangelnde Individualisierbarkeit in digitalisierten, distribuierten Systemen erschwert die rechtliche Zuordnung und damit die rechtliche Verantwortung und Kontrolle.[59] Rechtliche Steuerung baut in rechtsstaatlichen Demokratien allerdings auf individualisierbaren Personen auf, seien es natürliche oder juristische Personen,[60] sowie auf klarer Verantwortungszuschreibung.[61] Wer TrägerIn von Rechten und Pflichten ist, muss daher eindeutig festgelegt sein, will der Staat bzw das Recht seine Steuerungskraft nicht verlieren.[62]

In den Fällen, in denen die Individualisierbarkeit der Netzwerk-TeilnehmerInnen ausnahmsweise möglich ist,[63] fehlt diesen idR jeglicher Einfluss auf das System, weshalb sie schon aus Sachlichkeitserwägungen nicht verantwortlich gemacht werden können.[64] Die globale Ausrichtung der meisten digitalisierten, distribuierten Systeme[65] behindert die Verantwortungszuweisung zusätzlich. Im Ergebnis bedeutet dies, dass im Zentrum der Steuerungsbemühungen das Netzwerk,[66] der Code und dessen ProgrammiererInnen oder das Kollektiv stehen.[67] All dies erschwert die staatliche/rechtliche Steuerung oder Fremdbestimmung,[68] denn bleibt die ProgrammiererIn unbekannt, wie beim ursprünglichen Programmcode der Kryptowährung Bitcoin,[69] und verbreitet sich dessen Code einmal im Netz, übernimmt dieser die Steuerung der Netzwerk-Teilnehmenden, selbst wenn er veränderbar ist.

V. Digitalisierte distribuierte Systeme: Herausforderungen für demokratische Rechtssysteme

Blockchain-basierte Systeme sind idR globale Netzwerke, deren TeilnehmerInnen durch die Pseudonymisierung unbekannt bleiben, jedenfalls so lange sie sich im Netzwerk selbst bewe-

58 Siehe *Ehrke-Rabel/I. Eisenberger/Hödl/Pachinger/Schneider*, Kryptowährungen, Blockchain und Smart Contracts (Teil II), jusIT 2017, 132.

59 Vgl *Karnow*, Liability for Distributed Artificial Intelligences, Berkeley Technology Law Journal 1996, 155.

60 Siehe *Teubner,* Elektronische Agenten und große Menschenaffen: Zur Ausweitung des Akteursstatus in Recht und Politik, in *Becchi/Graber/Luminati* (Hrsg), Interdisziplinäre Wege in der juristischen Grundlagenforschung (2008) 2.

61 Siehe *Spiecker,* CR 2016, 700.

62 Siehe *Reuter*, Rechtsfähigkeit und Rechtspersönlichkeit: Rechtstheoretische und rechtspraktische Anmerkungen zu einem großen Thema, AcP 2007, (673) 681.

63 Siehe *Koops/Hildebrandt/Jaquet-Chiffelle,* Bridging the Accountability Gap: Rights for New Entities in the Information Society?, Minnesota Journal of Law, Science and Technology, 2010, 499.

64 Siehe *Spiecker,* CR 2016, 700; vgl auch *Beck,* Grundlegende Fragen zum rechtlichen Umgang mit der Robotik, JR 2009, 228.

65 Vgl *Johnson/Post,* Law and Borders – The Rise of Law in Cyberspace, Stanford Law Review, 1996, 1367.

66 Siehe *Ladeur,* Die Netzwerke des Rechts, in *Bommel/Tacke* (Hrsg), Netzwerke in der funktional differenzierten Gesellschaft (2010) 143.

67 Vgl *Ehrke-Rabel/I. Eisenberger/Hödl/Zechner*, ALJ 2017 (in Endredaktion).

68 Siehe *Koops/Hildebrandt/Jaquet-Chiffelle,* Minnesota Journal of Law, Science and Technology, 2010, 499.

69 Die Bitcoin Software wurde 2009 von einer Person(engruppe) unter dem Pseudonym „Satoshi Nakamoto" ins Leben gerufen (*Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System [2008]).

gen.[70] Unbekannt sind, wie zuvor bereits erwähnt, mitunter auch die ErfinderInnen des jeweiligen Systems; dies ist zumindest beim bislang bedeutendsten Blockchain-basierten System, der Kryptowährung Bitcoin, der Fall. In diesen softwarebasierten distribuierten Netzwerken setzen demzufolge die ProgrammiererInnen mit dem Code die normativen Standards.[71] Das für die Netzwerk-TeilnehmerInnen normativ relevante System ist kein staatlich gesetztes Recht, sondern ein von mitunter unbekannten EntwicklerInnen aufgestelltes Regelwerk.[72]

Anders als im Bereich demokratisch legitimierter Gesetzgebung geschieht dies beim Entwickeln Blockchain-basierter Systeme weitgehend ohne demokratische Legitimation und ohne demokratische Kontrolle, regelmäßig mit dem Ziel, (zentrale) staatliche Institutionen oder staatlich legitimierte Mittelspersonen zu beseitigen.[73] Besonders augenfällig ist die Verfolgung dieses libertären Ziels[74] bei den mittlerweile unzähligen Kryptowährungen, die explizit ein Finanzsystem ohne staatliche Legitimation und Kontrolle bezwecken.[75] Vom Standpunkt einer rechtsstaatlichen Demokratie aus betrachtet, sollten derartige Wünsche und Vorstellungen gesellschaftlich breit diskutiert werden und Wertentscheidung dieser Tragweite letztlich vom demokratisch legitimierten Gesetzgeber entschieden werden.[76]

Neben den demokratischen Legitimationsdefiziten setzt ein staatlich entgrenztes System, in dem die handelnden Personen unbekannt bleiben, rechtsstaatliche Demokratien vor zahlreiche Herausforderungen. Personen, an die staatliche/rechtliche Steuerung anknüpfen kann, sind regelmäßig nicht vorhanden, falls doch, sind sie aufgrund der mangelnden Einflussmöglichkeiten als rechtlicher Anknüpfungspunkt unzugänglich, staatliche Ingerenz- und Zugriffsmöglichkeiten diffundieren.[77] ProgrammiererInnen sind, selbst dann, wenn sie bekannt sein sollten, aufgrund der globalen Natur der Blockchain-basierten Systeme regelmäßig nicht greifbar. All dies verunmöglicht eine staatliche und rechtliche Steuerung dieser neuen Ordnungssysteme bislang. Zentrale rechtliche Institute, wie die Person, Zurechenbarkeit oder Verantwortlichkeit, verlieren ihre Wirkmächtigkeit.[78] Der Staat und das Recht können BürgerInnen und ihre Interessen zunehmend weniger schützen.[79]

Wenn die NetzwerkprogrammiererInnen und deren TeilnehmerInnen rechtlich kaum steuerbar sind,[80] bleibt die Frage, ob das technologische System ein rechtlicher Anknüpfungspunkt sein

70 Vgl *Ehrke-Rabel/I. Eisenberger/Hödl/Pachinger/Schneider*, jusIT 2017, 132.

71 Vgl *Spiecker*, CR 2016, 696; *Gruber/I. Eisenberger* in *I. Eisenberger/Lachmayer/G. Eisenberger* 51; *I. Eisenberger*, Das Trolley-Problem im Spannungsfeld autonomer Fahrzeuge: Lösungsstrategien grundrechtlich betrachtet, in *I. Eisenberger/Lachmayer/G. Eisenberger* (Hrsg), Autonomes Fahren und Recht (2017) 91.

72 Vgl *Lessig*, Code 120 ff; allgemein dazu *Robey*, Contract Management Magazine 2017, 18 (26) mit Verweis auf *Swan*, Blockchain: Blueprint for a New Economy (2015) 16 f.

73 Vgl *Nakamoto*, Bitcoin; *Atzori*, Blockchain Technology and Decentralized Governance: Is the State Still Necessary? SSRN 2015, 4 abrufbar unter https://ssrn.com/abstract=2709713 or http://dx.doi.org/10.2139/ssrn.2709713 (zuletzt abgefragt am 13. 11. 2017).

74 Siehe *Ehrke-Rabel/I. Eisenberger/Hödl/Pachinger/Schneider*, jusIT 2017, 87 (88).

75 Vgl *Huckle/White*, Future Internet (2016) 49. Siehe idZ ferner *Ehrke-Rabel/I. Eisenberger/Hödl/Pachinger/Schneider*, Kryptowährungen, Blockchain und Smart Contracts (Teil I), jusIT 2017, 87 sowie Teil II, jusIT 2017, 129.

76 Allgemein zur Notwendigkeit demokratisch legitimierte Gesetzgebung iZm neuen Technologien siehe *I. Eisenberger*, Innovation, insb 152 ff. Für eine zurückhaltende Regulierung im Bereich der Blockchain-Technologien spricht sich hingegen *Piska*, Kryptowährungen und ihr Rechtscharakter – eine Suche im Bermuda-Dreieck, ecolex 2017, 632 aus.

77 Vgl *Ehrke-Rabel/I. Eisenberger/Hödl/Pachinger/Schneider*, jusIT 2017, 129.

78 Vgl *Spiecker*, CR 2016, 696.

79 Vgl *D. Tapscott/A. Tapscott*, Blockchain 299.

80 Siehe idZ *Ehrke-Rabel/I. Eisenberger/Hödl/Zechner*, ALJ 2017 (in Endredaktion).

kann[81] und wenn ja, in welcher Form. Überlegungen, wie die elektronische Person[82] oder mit Rechtspersönlichkeit ausgestattete autonome Systeme,[83] stellen jedenfalls eine Herausforderung für den traditionellen Rechtsbegriff dar, wonach Recht von Menschen für Menschen gemacht ist[84] und in dem kein Platz für technologische Systeme als NormadressatInnen zu sein scheint. Mitunter ist es auch keine Frage rechtlicher Steuerung, sondern eine technologischer Normierung[85] und der Steuerung durch Design.[86] Die Zurückdrängung demokratisch-staatlicher Steuerung und damit konsensual errungener Werte liegt jedenfalls auf der Hand. Zum Schutz der Gesellschaft vor einer potentiellen Techno-Diktatur bedarf es neuer Mechanismen der Machtkontrolle und der Vorbeugung von Machtmissbrauch und eines Bewusstseinsbildungsprozesses innerhalb der neuen ProgrammiererInnen-Eliten.

VI. Resümee

Die Frage, wie selbst- oder fremdbestimmt Menschen in der zunehmend digitalisierten Welt sind, ist, wie gezeigt wurde, die falsche Fragestellung, denn Fehlverhalten, dass in einer digitalisierten und distribuierten Welt niemandem mehr zugerechnet werden kann und keine Verantwortung mehr auslöst, führt wohl zwangsläufig zu Machtmissbrauch, sei es durch Private oder durch den Staat. Das Netzwerk-Verhalten entzieht sich darüber hinaus aufgrund der weitgehend fehlenden rechtlichen Anknüpfungspunkte staatlicher Kontrolle. Es wäre daher zu fragen, woher wir in digitalisierten Systemen überhaupt wissen, wer bestimmt und wie wir die, die bestimmen, wieder sichtbar machen. Wie können wir die, die normative Standards setzen, zur Verantwortung ziehen und damit Macht kontrollieren und Missbrauch verhindern?[87] Können wir auch in digitalisierten und distribuierten Systemen zentrale rechtliche Anliegen, wie Verantwortung, Kontrolle und Machtbeschränkung effektuieren und wenn ja, mit rechtlichen oder anderen Instrumenten? So oder so sollte sich die Gesellschaft, aber auch die Rechtswissenschaft diesen Fragen im Sinne eines *„legal foresight"*[88] eher früher als später stellen und nicht erst, wenn technologische Systeme fest in unserer Gesellschaft verankert und kaum noch steuerbar sind.[89]

81 Vgl *Dulong de Rosnay*, Peer to party: Occupy the law, 5. 12. 2016, First Monday, http://journals.uic.edu/ojs/index.php/fm/article/view/7117/5658 (zuletzt abgefragt am 20. 7. 2017).

82 *Koops/Hildebrandt/Jaquet-Chiffelle*, Minnesota Journal of Law, Science and Technology 2010, 499; *Matthias*, Automaten als Träger von Rechten (2008); *Häusermann*, Autonome Systeme im Rechtskleid der Kapitalgesellschaft (2016) siehe unter: http://www.homburger.ch/fileadmin/publications/AUTOSYKG.PDF (zuletzt abgefragt am 10. 6. 2017); *Solum*, North Carolina Law Review 1992, 1231. Siehe ferner *Wiebe,* Die elektronische Willenserklärung (2002).

83 *Häusermann,* Autonome Systeme 5 ff.

84 Anstelle aller *Kelsen*, Reine Rechtslehre[2] 9.

85 Vgl *Reidenberg*, Texas Law Review 1998, 554; *Cockfield,* Manitoba Law Journal 2004, 405.

86 Siehe idZ *Schwarz-Plaschg/Kallhoff/I. Eisenberger*, Making Nanomaterials Safer by Design? NanoEthics 2017, 1 und die darin zitierte Literatur.

87 Vgl *Ehrke-Rabel/I. Eisenberger/Hödl/Zechner*, ALJ 2017 (in Endredaktion).

88 Vgl *Gruber/I. Eisenberger* in *I. Eisenberger/Lachmayer/G. Eisenberger* 67; *Bruckmüller/Schumann*, Automatisiertes und autonomes Fahren: Strafrechtliche Rahmenbedingungen in Österreich, in *I. Eisenberger/Lachmayer/G. Eisenberger* (Hrsg), Autonomes Fahren und Recht (2017) 123 (145).

89 Zur Akzeptanzsteigerung durch Demokratisierung siehe *I. Eisenberger*, Innovation 284 ff.

AUSTRIAN LAW JOURNAL

ISSN: 2409-6911

DOI: 10.25364/1.4:2017.2.9
www.austrian-law-journal.at

Der digitalisierte Steuerpflichtige

Tina Ehrke-Rabel,* Universität Graz

Kurztext: *Der digitalisierte Steuerpflichtige ist digitalisiert in seinem Wirtschaften und digitalisiert in seiner Interaktion mit der Finanzverwaltung. Digitale und digitalisierte Wirtschaftsmodelle stellen sowohl den Gesetzgeber als auch den Abgabenvollzug vor Herausforderungen, weil einerseits die physische Anknüpfung von Sachverhalten an staatliches Territorium nahezu unmöglich wird und andererseits staatliche Kontrolle von digitalen Wirtschaftsmodellen im derzeitigen System schwer möglich ist. Halten sich Steuerpflichtige an ihre Pflichten gegenüber der Finanzverwaltung, bietet die Digitalisierung jedoch Chancen für die Effizienzsteigerung des Vollzuges. Die Balance zwischen staatlicher Effizienz durch Digitalisierung und Schutz des Einzelnen vor übermäßigen Eingriffen in das Grundrecht auf Wahrung der Privatsphäre einerseits und dem Recht auf gute Verwaltung andererseits scheint derzeit jedoch noch nicht umfassend erreicht.*

Schlagworte: *digitaler Abgabenvollzug; Digitalisierung und staatliche Kontrolle; Recht auf gute Verwaltung; Effizienz des Vollzuges.*

I. Einleitung

Der Steuerpflichtige ist heute in mehrfacher Hinsicht „digitalisiert". Er ist digitalisiert, weil er selbst einen Großteil oder gar die Gesamtheit seiner Geschäftsprozesse, dh der Vorgänge, die letztendlich für eine Besteuerung relevant sind, digital abwickelt. Er ist digital, weil er einen Teil seines Privatlebens in die digitale Welt transportiert und dort dem Einblick dritter Privatrechtsakteure offenbart. Und er ist digitalisiert, weil er in Österreich seine Mitwirkungspflichten im Bereich des Steuerrechts vorwiegend digital abwickelt.

Aus steuerrechtlicher Sicht von Interesse ist der digitalisierte Steuerpflichtige in seiner digitalisierten Wirtschaftstätigkeit und in der Erfüllung seiner Mitwirkungspflichten gegenüber den Abgabenbehörden mittels digitaler Hilfsmittel.

II. Der digitalisierte Steuerpflichtige in seiner digitalisierten Wirtschaftstätigkeit

Die Digitalisierung hat gemeinsam mit dem Fall von Handelshemmnissen und damit der Globalisierung die Entfaltung von wirtschaftlichen Aktivitäten möglich gemacht, die unabhängig von der

* Univ.-Prof. Dr. Tina *Ehrke-Rabel* ist Leiterin des Instituts für Finanzrecht der Rechtswissenschaftlichen Fakultät der Universität Graz.

Fundstelle: *Ehrke-Rabel*, Der digitalisierte Steuerpflichtige, ALJ 2/2017, 150–159 (http://alj.uni-graz.at/index.php/alj/article/view/113).

physischen Anwesenheit auf einem bestimmten Markt (auf dem Territorium eines Staates) ist.[1] Für die Entfaltung wirtschaftlicher Tätigkeiten auf einem bestimmen Markt genügt heute vielfach die virtuelle Präsenz im Internet. Außerdem haben sich die Wirtschaftstätigkeiten als solche verändert. Was vor zehn Jahren noch als Verschaffung der Verfügungsmacht über einen körperlichen Gegenstand, etwa einer Musik-CD, bewirkt wurde, ist heute eine Dienstleistung, etwa in der Form der Zurverfügungstellung eines Musikdownloads über das Internet oder gar eines Abonnements bei einem Online-Musikkanal.

Die meisten Steuerrechtsbestimmungen, wie sie heute existieren, wurden in Zeiten entwickelt, in denen es noch kein Internet gab, in denen der Handel zwischen den Staaten noch stark beschränkt war und in denen der Dienstleistungssektor im Verhältnis zum Warensektor klein und vorwiegend auf Tätigkeiten beschränkt war, die eine physische Präsenz des Dienstleisters gegenüber dem Dienstleistungsempfänger vorausgesetzt haben. Dementsprechend knüpfen viele Steuerrechtsbestimmungen nach wie vor an physische Vorgänge an. So werden etwa Einkünfte eines ausländischen Warenanbieters im Inland nach den Regeln des internationalen Steuerrechts nur besteuert, wenn dieser Warenanbieter im Inland über eine feste Niederlassung, eine sog Betriebsstätte oder wenigstens einen ständigen Vertreter verfügt.[2] Vertreibt also heute ein außerhalb Österreichs ansässiger Händler seine Waren über ein Onlineportal in Österreich und liefert die Waren nicht über eine österreichische Betriebsstätte aus, unterliegen die aus den Verkäufen in Österreich erzielten Gewinne nicht der Ertragsteuer in Österreich.[3] Es bleibt bei der alleinigen Besteuerung im Ansässigkeitsstaat. Dies wird zunehmend als ungerecht empfunden. Eine Besteuerung im Inland würde eine Veränderung des internationalen Steuerrechts verlangen.[4] Überlegungen im Zusammenhang mit sog digitalen Betriebsstätten müssen jedoch erst zu Ende gedacht werden, scheitert die Anknüpfung an digitale Realitäten ohne physischen Bezugspunkt im Inland doch meistens am effizienten Vollzug in Österreich.

Aus umsatzsteuerrechtlicher Sicht etwa unterliegt dieser ausländische Warenanbieter ohne Betriebsstätte in Österreich nämlich der Umsatzsteuer in Österreich.[5] Leicht zu vollziehen ist dies jedoch nicht, wenn der ausländische Anbieter seine steuerrechtlichen Pflichten in Österreich nicht freiwillig erfüllt, dh selbst aktiv mitwirkt. Dass er dazu nach den allgemeinen Bestimmungen

1 OECD/G20 Base Erosion and Profit Shifting Project, Addressing the Tax Challenges of the Digital Economy, Action 1: 2015 Final Report, 15 f; *Kofler/Mayr/Schlager*, Digitalisierung und Betriebsstättenkonzept, RdW 2017, 369; *Ehrke-Rabel*, Steuervollzug im Umbruch, StuW 2015, 101.

2 Sog „Betriebsstättenregel"; dazu *Kofler/Mayr/Schlager*, RdW 2017, 369.

3 Dies ergibt sich aus den von Österreich großteils in Übereinstimmung mit Art 7 des Musterabkommens der OECD zur Vermeidung der Doppelbesteuerung abgeschlossenen bilateralen Doppelbesteuerungsabkommen. Nach Art 7 Abs 1 OECD-MA werden Unternehmensgewinne nur dann und nur insoweit (auch) im Quellenstaat besteuert, wenn und als sie einer dort gelegenen Betriebsstätte zuzurechnen sind. Die Betriebstätte wird in Art 5 OECD-MA definiert und setzt – verallgemeinernd definiert – eine gewissermaßen dauerhafte physische Präsenz im Quellenstaat voraus.

4 *Kofler/Mayr/Schlager*, RdW 2017, 379.

5 Das Umsatzsteuerrecht folgt grundsätzlich dem sog „Bestimmungslandprinzip". Danach unterliegen Warenlieferungen im Bestimmungsland der Umsatzsteuer. Ist der Empfänger der Lieferung ein Unternehmer, ist der Vollzug leicht möglich, weil die Steuerschuld grundsätzlich den empfangenden Unternehmer trifft (sog „innergemeinschaftlicher Erwerb" gem Art 1 Abs 1 UStG oder Einfuhr aus dem Drittland gem § 1 Abs 1 Z 2 UStG). Ist der Leistungsempfänger hingegen ein Privater und stammt die Ware aus dem übrigen Gemeinschaftsgebiet, so verlagert sich im Regelfall der Lieferort des ausländischen Lieferanten nach Österreich. Dieser muss dann österreichische Umsatzsteuer in Rechnung stellen, sich in Österreich registrieren und die Umsatzsteuer in Österreich abliefern (Art 3 Abs 3 ff UStG). Hält er sich nicht an seine Pflichten, ist es für die Finanzverwaltung schwer, die Verkürzung zu entdecken.

(der BAO[6] und des UStG[7]) verpflichtet ist, hilft wenig, wenn er nicht mitwirken will. Die Ausübung von Zwang durch die Abgabenverwaltung setzt nämlich zunächst voraus, dass die Abgabenverwaltung überhaupt von dem steuerpflichtigen Vorgang erfährt und wenn sie einmal davon erfahren hat, kann Zwang im Ausland nur im Wege der Amtshilfe ausgeübt werden. Diese wiederum setzt entsprechende Rechtsgrundlagen und die Kooperation des Ansässigkeitsstaates des betroffenen Steuerpflichtigen voraus.[8] Der Gesetzgeber hat nicht viele Möglichkeiten, dieses Vollzugsdefizit zu überwinden. Ein wirksames Instrument ist immerhin die Einbindung dritter „Mitwisser" in die Informationsbeschaffung. So kann man Vertragspartner der ausländischen Unternehmer, so sie selbst Unternehmer sind, zur Mitteilung über bestimmte Vorgänge an die Finanzverwaltung verpflichten[9] oder auch einen Abzug der Steuer durch den inländischen Vertragspartner vorsehen.[10] Sind die Vertragspartner der ausländischen Unternehmer jedoch Konsumenten, wird es aus verfassungsrechtlicher Sicht schwierig, ihnen Informationspflichten gegenüber der Abgabenverwaltung betreffend einen Dritten aufzuerlegen.[11] Im Versandhandel etwa hat sich der Gesetzgeber damit beholfen, dass das Briefgeheimnis nicht mehr umfassend gilt: Für Zoll- und Umsatzsteuerzwecke darf die Verwaltung Pakete öffnen und bestimmte Auskünfte vom Postdienstleister verlangen.[12] Aber auch Pakete kann man nur öffnen, wenn man weiß, dass sie da sind.

Wenn der Umsatzsteuer- und der Glücksspielgesetzgeber auf die Digitalisierung reagiert haben, indem sie digital erbrachte Dienstleistungen dort der Umsatzsteuer bzw der Glücksspielabgabe unterwerfen, wo – untechnisch gesprochen – der Konsum dieser Dienstleistung stattfindet,[13] dann gelingt das auch nur, wenn mit gesetzlichen Vermutungen gearbeitet wird[14] oder würde[15]. Wer seine Dienstleistungen über das Netz anbietet, kann nämlich niemals mit Sicherheit feststellen, wo sich der Leistungsempfänger befindet, wenn er die Dienstleistung in Anspruch nimmt. Noch schwieriger ist es für die Finanzverwaltung, die Rechtsmäßigkeit der Angaben des Steuer-

6 §§ 115 ff BAO.

7 § 21 UStG.

8 Innerhalb der EU sollte das Problem insoweit entschärft sein, als es EU-weit einheitliche und umfassende Amtshilfeverpflichtungen gibt, die im Bereich der Umsatzsteuer in der EU-Amtshilfeverordnung VO (EU) 904/2010 des Rates vom 7. 10. 2010 über die Zusammenarbeit der Verwaltungsbehörden und die Betrugsbekämpfung auf dem Gebiet der Mehrwertsteuer, ABl L 2010/268, 1 und RL 2011/16/EU über die Zusammenarbeit der Verwaltungsbehörden im Bereich der Besteuerung, ABl L 2011/64, 1, umgesetzt durch das EU-Amtshilfegesetz (kurz: EU-AHG). Praktisch erweist sich die Amtshilfe bisweilen jedoch aus verschiedenen Gründen als schwerfällig.

9 Das EStG sieht an verschiedenen Stellen Mitteilungspflichten Dritter vor (zB § 109a oder § 109b EStG).

10 Einen Quellensteuerabzug statuieren etwa § 93 EStG iZm bestimmten Kapitalerträgen oder § 99 EStG iZm bestimmten Zahlungen an ausländische VertragspartnerInnen.

11 Zu den verfassungsrechtlichen Grenzen zulässiger Inpflichtnahme in Steuersachen zur vergleichbaren deutschen Rechtslage *Drüen*, Die Indienstnahme Privater für den Vollzug von Steuergesetzen (2012).

12 § 27 Abs 5 und Abs 6 UStG.

13 Gem § 3a Abs 13 UStG werden elektronisch erbrachte Dienstleistungen an Nicht-Unternehmer (Konsumenten) dort ausgeführt und sind dort steuerbar, wo der Leistungsempfänger seinen Wohnsitz, Sitz oder gewöhnlichen Aufenthalt im Drittlandsgebiet hat. Nach § 57 Abs 2 unterliegen elektronische Lotterien, die nicht glücksspielrechtlich konzessioniert sind, in Österreich einer Glücksspielabgabe, wenn die Teilnahme an der elektronischen Ausspielung vom Inland aus erfolgt.

14 Das UStG arbeitet mit gesetzlichen Vermutungen, die widerlegbar sind (Art 24a ff Durchführungsverordnung (EU) 282/2011 des Rates vom 15. 3. 2011 zur Festlegung von Durchführungsvorschriften zur RL 2006/112/EG über das gemeinsame Mehrwertsteuersystem, ABl L 2011/77, 1 (kurz: MwSt-DVO). Diese Bestimmungen werden unionsweit einheitlich angewandt.

15 Im Unterschied zum Umsatzsteuerrecht arbeitet das GSpG nicht mit gesetzlichen Vermutungen. Die Glücksspielabgabe auf elektronische Lotterien iSd § 12a GSpG wird in Österreich erhoben, wenn *„die Teilnahme vom Inland aus erfolgt"* (§ 57 Abs 2 GSpG). Das Problem liegt hier darin, dass weder der Steuerpflichtige, nämlich der Anbieter der Lotterie, noch die Finanzverwaltung selbst in der Lage sind, mit vernünftigen Mitteln zu überprüfen, ob der Spieler von Österreich aus an der elektronischen Lotterie teilgenommen hat (dazu jüngst *Gunacker-Slawitsch*, Online-Glücksspiel und Beweismaß, taxlex 2017 [in Druck]).

pflichtigen zu überprüfen. Das Steuerrecht ist hier vor die Herausforderung gestellt, nicht Regelungen zu schaffen, die mangels Kontrollierbarkeit das Steuerzahlen zur Beliebigkeit machen.

Die Entwicklungen sind noch lange nicht zu Ende: Auch wenn gute Chancen bestehen, dass klassische Fälle digitalen Wirtschaftens in irgendeiner Weise steuerrechtlich in den Griff bekommen werden, entwickelt die Digitalisierung immer neue Wirtschaftsmodelle. Die größte Herausforderung in diesem Zusammenhang sind sicherlich dezentrale distribuierte Systeme, die Transaktionen im Netz ohne Mittelsmänner erlauben, virtuelle Werte schaffen und im Regelfall mit kryptographischer Verschlüsselung arbeiten.[16]

III. Der Steuerpflichtige im digitalisierten Abgabenverfahren

Steuern dienen der Finanzierung der Staatsaufgaben. In Staaten, die sich – wie die Mitgliedstaaten der EU – zur sozialen Marktwirtschaft bekennen (Art 3 EUV), haben sie außerdem eine Umverteilungsfunktion, indem sie Transferleistungen von den sehr leistungsfähigen Menschen zu jenen Menschen ermöglichen, denen aus verschiedenen Gründen die Sicherung einer lebenswerten Existenz selbst nicht möglich ist.

Steuerrecht ist Eingriffsrecht. Es ist Verwaltungsrecht und da Steuern das Privateigentum des Einzelnen beschneiden, hat ihre Erhebung dem Gesetzesvorbehalt des Grundrechts auf Privateigentum gerecht zu werden. Steuern dürfen also nur aufgrund der Gesetze erhoben werden (Art 18 B-VG). Dies trifft sowohl für das materielle Steuerrecht zu als auch für jene Regeln, die die Ermittlung besteuerungserheblicher Sachverhalte, sowie die Festsetzung und Eintreibung der Steuerschulden betreffen. Steuern sollen außerdem gerecht sein. In den meisten westlichen Demokratien werden jene Steuern als am gerechtesten empfunden, die den einzelnen nach seiner individuellen wirtschaftlichen Leistungsfähigkeit belasten.[17] Bei der Bewertung dieser individuellen Leistungsfähigkeit spielen neben den Aufwendungen, die der einzelne für den Erwerb seines Einkommens zu tragen hat (sog „objektives Nettoprinzip"),[18] auch persönliche Umstände eine große Rolle. Dazu zählen etwa der Umstand, dass für Kinder gesorgt werden muss, außergewöhnliche Umstände, etwa Schicksalsschläge im privaten Umfeld, die erhöhte Kosten der privaten Lebensführung verursacht haben, oder Krankheitskosten, die von keiner Versicherung getragen werden (sog „subjektives Nettoprinzip").[19] Auch bloße Rechtsverkehrssteuern, wie etwa die Grunderwerbsteuer, also die Steuer auf die Übertragung von unbeweglichem Vermögen, sollen aus politischen Gerechtigkeitserwägungen etwa zwischen entgeltlichen und unentgeltlichen Übertragungen differenzieren. Schließlich sollen bestimmte Vorgänge aus bestimmten rechtspolitischen Erwägungen nicht oder geringer besteuert werden (zB die unentgeltliche Übertragung von Grundstücken im Rahmen einer Betriebsübergabe oder die Begründung von Miteigentum im Zusammenhang mit einer Ehe). Die Liste ließe sich unendlich fortsetzen. Was sie deutlich machen

16 Dazu in dieser Ausgabe *I. Eisenberger*, Digitalisierung und Selbstbestimmung, ALJ 2/2017, 140; *Ehrke-Rabel/I. Eisenberger/Hödl/Pachinger/Schneider*, Kryptowährungen, Blockchain und Smart Contracts: Risiken und Chancen für den Staat (Teil I), JusIT 2017, 87; *Ehrke-Rabel/I. Eisenberger/Hödl/Zechner*, Bitcoin-Miner als Prosumer, ALJ 2017 (in Endredaktion).

17 *Doralt/Ruppe*, Steuerrecht I[11] (2013) Tz 22 ff; *Beiser*, Steuern[14] (2016) Tz 6.

18 Eine Person, die ihren Lebensunterhalt durch den Verkauf von selbstproduzierten Gegenständen bestreitet, wird höhere Aufwendungen zur Herstellung dieser Gegenstände haben als jemand, der seinen Lebensunterhalt durch die Erbringung von Beratungsleistungen sichert.

19 *Doralt/Ruppe*, Steuerrecht I[11] Tz 25 f.

soll, ist, dass das Steuerrecht an Lebenssachverhalte anknüpft, die vielfach komplex sind und die dem Auge des Staates zunächst nicht ohne weiteres zugänglich sind.

Obwohl die Abgabenbehörden ganz im Sinne ihrer Zuordnung zur Eingriffsverwaltung die abgabepflichtigen Fälle zu erforschen und die tatsächlichen und rechtlichen Verhältnisse von Amts wegen zu ermitteln haben, die für die Abgabenpflicht und die Erhebung der Abgaben wesentlich sind (§ 115 BAO), sind die Abgabepflichtigen ihrerseits gehalten, die für den Bestand und den Umfang einer Abgabepflicht oder für die Erlangung abgabenrechtlicher Begünstigungen maßgeblichen Umstände offenzulegen (§ 119 Abs 1 BAO). Die Offenlegung muss vollständig und wahrheitsgemäß erfolgen. Damit Steuern überhaupt im Sinne der Gesetze erhoben werden können, muss der einzelne Steuerpflichtige umfassend mitwirken und der Finanzverwaltung eine Vielzahl personenbezogener Daten zur Verfügung stellen. Personenbezogene Daten sind nämlich alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar werden Personen angesehen, die direkt oder indirekt, insb mittels Zuordnung zu einer Kennung wie etwa einem Namen, identifiziert werden können (Art 4 Z 1 DSG-VO; § 4 Z 1 DSG 2000).

Dass im Besteuerungsverfahren eine Vielzahl personenbezogener Daten übermittelt werden, ist zu einem Großteil unserem Gerechtigkeitskonzept geschuldet. Eine Steuer, die sich etwa nach der Anzahl der Fenster bemisst, wäre wesentlich einfacher zu erheben und würde wesentlich weniger personenbezogener Daten des einzelnen bedürfen, würde aber den modernen Gerechtigkeitsvorstellungen in keiner Weise Rechnung tragen.

Da Steuern jeden treffen, ist Steuerrecht Massenfallrecht in der deutschen Ausdrucksweise, auf Österreichisch handelt es sich schlicht um ein Massenverfahren. Dieses Massenverfahren war mit eingeschränkten staatlichen Ressourcen bereits im Jahr 1965 nicht auf denselben Wegen zu bewältigen wie andere Bereiche des Eingriffsrechts. Vor diesem Hintergrund hegte der VfGH bereits im Jahr 1965 keine Bedenken dagegen, dass die Rechtskraft von Bescheiden im Abgabenrecht eine schwächere Ausprägung erfahren hat als im allgemeinen Verwaltungsrecht.[20] Er hielt es für gleichheitsrechtlich unbedenklich, dass die Abgabenbehörden einen Abgabenbescheid bis zum Ablauf eines Jahres nach dessen Verkündung nach jeder Richtung, also auch zu Lasten des Einzelnen, ändern dürfen.[21] Das ist bis heute so geblieben und die Instrumente haben sich angesichts der digitalen Möglichkeiten weiterentwickelt.[22]

Im Unterschied zu *Kirchhof* halte ich das für die einzige realistische Möglichkeit, den Steuervollzug effizient auszugestalten. Mit *Kirchhof* bin ich aber der Meinung, dass bei der Ausgestaltung eines digitalen Vollzugs das Legalitätsprinzip und die Grundrechte, insb das Recht auf Schutz des Privatlebens bzw das Grundrecht auf Datenschutz zu beachten sind. Anders als *Kirchhof* sehe ich gerade das Grundrecht auf Datenschutz innerhalb der EU nicht durch den automatischen Informationsaustausch von Finanzdaten gefährdet oder gar verletzt.[23]

Um die „Massenhaftigkeit" des Steuerrechts im Vollzug zu bewältigen, dienten schon zu Zeiten, zu denen die Digitalisierung nicht existierte, insb Abgabenerklärungen, Anmeldungen, Anzeigen, (...) der Offenlegung im Rahmen der Mitwirkungspflichten (§ 119 Abs 2 BAO). Die Abgabenerklärung

20 VfGH G 24/64 VfSlg 4986 = JBl 1966, 217.
21 VfGH G 24/64 VfSlg 4986 = JBl 1966, 217; ausdrücklich bestätigt durch VfGH G 5/88 VfSlg 11.865.
22 *Ehrke-Rabel*, Rechtskraft bei inhaltlich zusammenhängenden Bescheiden im Abgabenverfahren, in *Holoubek/Lang* (Hrsg), Rechtskraft (2007) 216; *Ehrke-Rabel/Hödl*, Steuerbescheid und behördliches Profiling, DAKO 2017, 59.
23 *Kirchhof*, Der digitalisierte Steuerzahler, ALJ 2/2017, 125.

stellt also das Standardinstrument zur Erfüllung abgabenrechtlicher Offenlegungspflichten dar. Soweit dafür amtliche Vordrucke vorgesehen sind, sind die Abgabenerklärungen unter Verwendung dieser Vordrucke abzugeben (§ 133 Abs 2 BAO). Im Fall der automationsunterstützten Datenübertragung, zu der die Abgabepflichtigen jedenfalls für die aufkommensstärksten Steuerarten[24] (Einkommensteuer,[25] Lohnsteuer,[26] Körperschaftsteuer,[27] Umsatzsteuer[28]) verpflichtet sind,[29] entfällt zwar die Verpflichtung zur Verwendung des amtlichen Vordruckes,[30] doch wird diese durch die Verpflichtung zur Verwendung der wenig individuelle Spielräume aufweisenden, elektronischen Eingabemaske ersetzt.[31] Der Steuerpflichtige stellt in diesem Verfahrensstadium zunächst den besteuerungserheblichen Sachverhalt fest, subsumiert ihn selbständig unter die einschlägigen Steuerrechtsnormen und hält das Ergebnis dieses Feststellungs- und Subsumtionsprozesses schließlich in Zahlen komprimiert in den standardisierten Steuererklärungen fest. Diese Erklärungen eröffnen keinerlei Spielräume für individuelle Erklärungen und werden auch elektronisch an das Finanzamt übermittelt.[32] Außerdem werden den Finanzbehörden von Dritten Daten über steuererklärungspflichtige Personen weitergeleitet.[33] Finden sich diese Daten in den Steuerklärungen der betroffenen erklärungspflichtigen Personen nicht wieder, kann die Finanzbehörde die Verschleierung bestimmter Einkünfte mit größerer Wahrscheinlichkeit erkennen.

Sämtliche Materiengesetze, welche die elektronische Übermittlung der Steuererklärungen oder sonstiger für die Besteuerung erheblicher Informationen verlangen, ermächtigen den Bundesminister für Finanzen (BMF) einerseits dazu, die Verwendung einer bestimmten Übermittlungsstelle per Verordnung vorzuschreiben und andererseits, das Verfahren und den Inhalt der elektronischen Übermittlung per Verordnung zu regeln.[34] In Umsetzung dieser Bestimmungen hat der BMF die sog FinanzOnline-Verordnung[35] und die FinanzOnline-Erklärungsverordnung[36] erlassen. Beide Verordnungen sind sehr technisch und regeln in erster Linie, wie und durch wen die erforderlichen Daten zu übermitteln sind.

24 *BMF*, Die österreichische Steuer- und Zollverwaltung, Geschäftsbericht 2015, 2, https://www.bmf.gv.at/publikationen (zuletzt abgerufen am 27. 11. 2017).

25 § 42 Abs 1 UAbs 2 EStG.

26 § 84 Abs 1 Z 2 EStG.

27 § 24 Abs 3 Z 1 KStG.

28 § 21 Abs 1 UAbs 4 UStG; § 21 Abs 4 UAbs 2 UStG.

29 Nach § 42 Abs 1 UAbs 2 EStG hat die Übermittlung der Einkommensteuererklärung elektronisch zu erfolgen. Nur wenn dem Steuerpflichtigen die elektronische Übermittlung mangels technischer Voraussetzungen unzumutbar ist, hat die Übermittlung unter Verwendung des amtlichen Vordrucks zu erfolgen. Auch wenn die Lohnsteuer vom Arbeitgeber monatlich selbst zu berechnen und abzuführen ist (§§ 78 ff EStG), haben Arbeitgeber einmal jährlich den Lohnzettel elektronisch zu übermitteln (§ 84 Abs 1 Z 2 EStG). Die Körperschaftsteuererklärung ist gem § 24 Abs 3 Z 1 KStG – außer im Fall der Unzumutbarkeit – elektronisch zu übermitteln. Dasselbe gilt für die Umsatzsteuer (§ 21 Abs 1 UAbs 4 UStG).

30 § 133 Abs 2 BAO.

31 Dazu schon *Ehrke-Rabel/Gunacker-Slawitsch*, Governance im Steuerrecht, SWK 2014, 1054.

32 *Ehrke-Rabel/Gunacker-Slawitsch*, SWK 2014, 1054; *Ehrke-Rabel/Gunacker-Slawitsch*, Die Bedeutung von Governance für das Steuerrecht, ALJ 1/2014, 99.

33 ZB § 109a EStG, aber auch diverse automatische Datenübermittlungen aus dem Ausland auf der Grundlage der europäischen und internationalen Informationsaustauschbestimmungen.

34 § 21 Abs 1 UAbs 4 und UAbs 5 UStG; § 24 Abs 3 Z 1 KStG; § 84 Abs 1 Z 4 EStG; § 42 Abs 1 UAbs 2 EStG.

35 Verordnung des BMF über die Einreichung von Anbringen, die Akteneinsicht und die Zustellung von Erledigungen in automationsunterstützter Form (FinanzOnline-Verordnung 2006, FOnV 2006) BGBl II 2006/97 idF BGBl II 2016/46.

36 Verordnung des BMF über die elektronische Übermittlung von Steuererklärungen sowie von Jahresabschlüssen und anderen Unterlagen anlässlich der Steuererklärung (FinanzOnline-Erklärungsverordnung – FOnErklV) BGBl II 2016/512 idF BGBl II 2016/310.

Wie die Finanzbehörde die elektronisch und standardisiert übermittelten Daten behandelt, ist gesetzlich nicht besonders geregelt. Es gelten vielmehr die allgemeinen Bestimmungen, die weitgehend aus Zeiten weit vor der Digitalisierung stammen:[37] Die Abgabenerklärungen sind von der Abgabenbehörde zu prüfen, bei Zweifeln sind Ergänzungsaufträge, bei Bedenken gegen die Richtigkeit der Abgabenerklärung Bedenkenvorhalte zu erteilen (§ 161 BAO). Will die Behörde von der Abgabenerklärung abweichen, hat sie dem Steuerpflichtigen rechtliches Gehör zu gewähren (§ 161 Abs 3 und § 115 Abs 2 BAO). Angesichts der Massenhaftigkeit des Verfahrens und der bereits erwähnten beschränkten staatlichen Ressourcen ist eine Überprüfung aller Steuerpflichtigen im Sinne einer „100%-Kontrolle" unmöglich.[38]

Die elektronische Übermittlung der Steuerdaten in absolut standardisierter Form ermöglicht jedenfalls eine elektronische und automationsunterstützte Verarbeitung im weitesten Sinn. Diese Form der Übermittlung macht es nämlich nicht unbedingt notwendig, dass die Abgabenbehörde in der Form eines Menschen die Erklärung prüft. Gerade der Vergleich mit Eingaben in vorangegangenen Veranlagungszeiträumen oder auch der Vergleich mit Daten von anderen Steuerpflichtigen in vergleichbaren Situationen kann technisch durch einen Algorithmus vorgenommen werden. Ist der Algorithmus der Behörde als Hilfsinstrument zurechenbar, vollzieht er behördliches Handeln. Da es sich bei den von den Steuerpflichtigen übermittelten Daten um personenbezogene Daten handelt, ist der hier beschriebene Datenabgleich als „Verarbeitung" von Daten iSv Art 4 Z 2 DSG-VO (§ 4 Z 9 DSG 2000) zu qualifizieren. Dabei handelt es sich nämlich um einen mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (Art 4 Z 2 DSG-VO).

Dass die Finanzverwaltung die Daten sammelt, aufbewahrt und überprüft, ist gesetzlich vorgesehen. Gesetzlich nicht vorgesehen ist, wie sie diese Überprüfung durchführt. Die Datenverarbeitung ist auch zweifelsohne für die Wahrung einer Aufgabe im öffentlichen Interesse, nämlich für die Sicherung des Steueraufkommens und für die Wahrung der gleichmäßigen Steuererhebung erforderlich. Sie ist daher rechtmäßig, wenn sie gesetzlich verankert ist (Art 6 Abs 3 lit a DSG-VO; § 7 Abs 1 DSG 2000). Nähere Bestimmungen über die Art der Verarbeitung, die Dauer der Aufbewahrung etc können nach Art 6 Abs 2 DSG-VO vorgesehen werden, sind aber nicht absolut notwendig. Dass das österreichische Recht diesbezüglich nichts Näheres vorsieht, ist somit aus datenschutzrechtlicher Sicht unbedenklich. Letztendlich – so könnte man jedenfalls rational argumentieren – sind die Daten ohnehin bei der Finanz, die durch das Steuergeheimnis nach § 48a BAO zur Verschwiegenheit über die ihr zur Kenntnis gelangten Informationen und nach § 161 BAO zur Kontrolle der Steuererklärungen verpflichtet ist. Wird die Kontrolle automationsunterstützt durchgeführt, dann ist dies bei entsprechend sachkundiger Gestaltung des Algorithmus der Gleichmäßigkeit der Besteuerung sogar zuträglicher, weil der Algorithmus – anders als der prüfende Mensch – in der Gewissenhaftigkeit seiner Überprüfungen nie durch menschliche Bedürfnisse (wie Schlaf, Nahrung) beeinträchtigt werden kann.

37 § 161 BAO lässt sich auf § 205 der Reichsabgabenordnung aus dem Jahr 1931 zurückführen.
38 VfSlg 4986/1965.

Fest steht aber, dass Veranlagungsabgaben jedenfalls[39] durch einen Bescheid festgesetzt werden. Anders als im allgemeinen Abgabenverfahren bedürfen automationsunterstützt erlassene Bescheide weder einer Unterschrift noch einer Beglaubigung und gelten, wenn sie weder eine Unterschrift noch eine Beglaubigung aufweisen, als durch den Leiter der auf der Ausfertigung bezeichneten Abgabenbehörde genehmigt (§ 96 BAO).[40] Der VwGH hält die „Freigabe" des Bescheides durch einen Organwalter für ausreichend, um die Rückführung der Ausfertigung auf den Willen eines Organwalters der Behörde zu ermöglichen.[41] Das Abgabenrecht lässt also die automationsunterstützte Bescheidausfertigung ohne weiteres zu.

Die Überprüfung der übermittelten Daten kann also durchaus durch eine Maschine vorgenommen werden. So könnte eine Unterscheidung zwischen „wenig auffälligen" und „auffälligen" Steuererklärungen getroffen werden.[42] Angesichts der im Verhältnis zum allgemeinen Verwaltungsverfahren umfassenden Rechtskraftdurchbrechungsmöglichkeiten könnten also in den wenig auffälligen Fällen auf konkrete Nachforschungen verzichtet und zunächst ein erklärungskonformer Bescheid automatisch erlassen werden. Dies hätte den Vorteil, dass der Staat schneller zu seinem Geld kommt. Die knappen Humanressourcen könnten dann gezielt in den auffälligen Fällen eingesetzt werden. Gesetzlich explizit geregelt ist eine solche Datenverarbeitung derzeit nicht. Die BAO sieht nur vor, dass die Finanzbehörde eine elektronische Dokumentation (ein Dokumentationsregister) anlegen (§ 114 Abs 2 BAO) und Anbringen und andere das Verfahren betreffende Anbringen mit automationsunterstützter Datenverarbeitung erfassen darf (§ 114 Abs 3 BAO). Außerdem ermächtigt § 114 Abs 4 BAO die Abgabenbehörden, Daten automationsunterstützt zu verarbeiten, die ihnen im Rahmen ihrer Zuständigkeit entweder aufgrund gesetzlicher Verpflichtungen oder freiwillig überlassen oder die sonst bei der Vollziehung von Abgabenvorschriften und bei der Wahrnehmung ihrer Aufgaben gewonnen werden. Die Datenverarbeitung ist nur zulässig, soweit sie erforderlich und verhältnismäßig ist. Das bedeutet, dass die Datenverarbeitung zur Verhinderung und zur Aufklärung abgabenrechtlicher Gesetzesverletzungen geeignet, erforderlich und angemessen sein muss. Ob diese sehr generelle Ermächtigung als hinreichende Grundlage für einen Datenabgleich und eine Vorselektion in der beschriebenen Form taugt, darf hier zumindest in Frage gestellt werden.

Fest steht, dass Steuerbescheide vielfach zunächst erklärungskonform und immer automationsunterstützt erlassen werden.[43] In seltenen Fällen ergehen nach Übermittlung der Steuererklärung und vor Erlassung des Steuerbescheides behördliche Nachfragen. Dass elektronisch eingereichte Steuererklärungen bereits vor Erlassung des Bescheides einem automatisierten Überprüfungsprozess unterworfen werden, erscheint also nicht unwahrscheinlich. Aus grundrechtlicher und insb datenschutzrechtlicher Sicht dürfte dieses Vorgehen auch unbedenklich sein, solange der

39 Bei Selbstbemessungsabgaben setzt die Entrichtung der Abgabenschuld durch den Steuerpflichtigen, ohne dass die Finanzverwaltung in irgendeiner Form an der Festsetzung mitgewirkt hat, den (vorläufigen) Endpunkt.

40 Nach den ErläutRV 108 BlgNR 17. GP 40, die zur Einführung des § 96 letzter Satz BAO führten, erging bereits im Jahr 1987 eine Vielzahl von Bescheiden in einem „vollautomatisierten" Verfahren. Die gesetzliche Vermutung an Stelle des Unterschriftserfordernisses wurde daher eingeführt, um die von VfGH und VwGH geforderte Unterschrift als Willensbekundung des Organwalters der zuständigen Behörde zu ersetzen. Dazu schon *Holzinger*, Der „Computerbescheid" in der Judikatur der Gerichtshöfe des öffentlichen Rechts, in FS W. Rosenzweig (1988) 193 (194).

41 VwGH 24. 11. 2011, 2008/15/0205; 16. 12. 2010, 2009/15/0002; 14. 12. 2006, 2005/14/0014.

42 *Ehrke-Rabel/Hödl*, Profiling, DAKO 2017, 59 f.

43 *Rombold*, § 299 BAO als kleine Schwester der „Abgabenfestsetzung unter Vorbehalt", SWK 2005, 910; *Gunacker-Slawitsch*, Auskunftspflicht als Grundlage für die „Nachbescheidkontrolle"? RdW 2011, 699 (711).

automatisiert erlassene Bescheid die vom Steuerpflichtigen übermittelten Daten ohne Abweichungen übernimmt (sog „erklärungskonforme Veranlagung"). Nur dann, wenn von den übermittelten Daten abgewichen werden soll, dann verpflichtet bereits das einfache Recht zur Wahrung des Parteiengehörs, wenngleich der Schutz gegen Verstöße ein relativ geringer ist, weil Verstöße im Rechtsmittelverfahren saniert werden können.[44] Im Anwendungsbereich des Unionsrechts gilt dies jedenfalls auch nach dem aus den Rechtstraditionen der Mitgliedstaaten abgeleiteten Recht auf gute Verwaltung.[45]

Einer automatischen Bescheidausfertigung in Abweichung von den durch den Abgabepflichtigen übermittelten Daten dürfte – ohne entsprechend gesetzliche Ausgestaltung – aber auch das Grundrecht auf Datenschutz entgegenstehen: Nach Art 22 Abs 1 DSG-VO hat die betroffene Person das Recht, nicht einer auf einer ausschließlich automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Diese Beschränkung steht unter Gesetzesvorbehalt und dürfte durchbrochen werden, wenn sie gesetzlich vorgesehen ist und die entsprechenden Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der Partei enthalten (Art 22 Abs 2 lit b DSG-VO). § 114 Abs 4 BAO wäre dafür jedenfalls keine hinreichende Grundlage.

Außerdem könnten auch im Fall bereits erlassener Bescheide die zugrunde gelegten Daten einer Datenverarbeitung unterworfen werden, um die Auswahl von Betriebsprüfungsfällen effizient auf Risikofälle zu konzentrieren. Dass dies in Österreich bereits geschieht, deutet ein Hinweis auf der Homepage des BMF an. Unter dem Stichwort *„Predictive Analytics Competence Center (PACC)"* findet sich folgende Aussage:

> *„Das PACC soll eine risikoorientierte Einsatzlenkung ausgehend von einer nach neuesten wissenschaftlichen Methoden durchgeführten Risikobeurteilung der Abgabenprozesse und damit verbundenen Vorhersagen der erforderlichen Kontroll- und Prüfungsmaßnahmen verantworten und durch eine ganzheitliche Evaluierung der Ergebnisse dieser Maßnahmen auch zu deren Optimierung beitragen. Mit mathematisch-statistischen Analysemethoden soll die Trefferquote bei der Fallauswahl in der Betrugsbekämpfung in den nächsten Jahren erhöht werden.*
>
> *Das Ziel der Nutzung von Big Data-Informationen sind datengetriebene Entscheidungen. Daher werden innovative und kreative Analysemethoden erforderlich, wie zB Datamining, Predictive Analytics, Simulationen und Szenarienforschung […]."*

Wie Predictive Analytics in der österreichischen Finanzverwaltung funktioniert, erläutert *Setnicka*[46] im Detail.

Bei diesen Analysen kann es sich durchaus um sog „Profiling" handeln. Darunter versteht die DSG-VO *„jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirt-*

44 *Ehrke-Rabel* in *Doralt/Ruppe* (Hrsg), Steuerrecht II[14] (2014) Tz 1304.

45 Dazu *Gunacker-Slawitsch*, Das Grundrecht auf eine „gute Verwaltung" im Abgabenverfahren (Teil 2), ÖStZ 2015, 301.

46 Predictive Analytics in der österreichischen Finanzverwaltung, in *Mayr/Pinzger* (Hrsg), INFORMATIK 2016: Lector Notes in Informatics (LNI), Gesellschaft für Informatik (2016) 629.

schaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen".[47] An anderer Stelle macht die DSG-VO deutlich, dass es sich bei Profiling um eine systematische und umfassende Bewertung handelt.[48] Profiling reicht also weiter als eine „einfache" Datenverarbeitung.[49] Auf diese Weise ermöglicht die automatisierte Verarbeitung von Daten im Rahmen des Profiling die *Analyse und Vorhersage* bestimmter höchstpersönlicher Lebens- und Themenbereiche von Menschen.[50] Angesichts der umfangreichen Daten, die der einzelne im Rahmen seiner Steuererklärungspflichten zur Festsetzung der sachgerechten Steuer preiszugeben hat, würden ein umfassendes Profiling ermöglichen.

Ob die Abgabenverwaltung in diesem Zusammenhang derzeit den datenschutzrechtlichen Anforderungen gerecht wird, darf angesichts der kaum existenten expliziten Rechtsgrundlagen, zumindest bezweifelt werden.

IV. Conclusio

Dass die Instrumente der Digitalisierung nicht vom Steuerpflichtigen im Rahmen seiner wirtschaftlichen Aktivitäten, sondern auch vom Staat im Rahmen seiner Pflichten verwendet werden, ist mehr als legitim. Es ist für die Erfüllung des gesetzlichen Auftrages, die Gleichmäßigkeit der Besteuerung zu sichern, sogar dringend notwendig. Dass eine Vereinfachung des materiellen Steuerrechts wünschenswert wäre und sowohl den Vollzug erleichtern als auch die Befolgungskosten für den Steuerpflichtigen reduzieren würde, ist unbestritten. Wahrscheinlicher als eine drastische Vereinfachung des materiellen Rechts erscheint jedoch die Gestaltung eines modernen Abgabenverfahrens, das moderne Instrumente des Vollzugs auf ein verfassungsrechtlich gesichertes Fundament des Vollzugs setzt. Auf verfassungsrechtliche Absicherung sollte Bedacht genommen werden. Nicht jedes technische Hilfsmittel, das menschliche Arbeit ersetzt, kann im Verwaltungsvollzug ohne weitere gesetzliche Fundierung eingesetzt werden.

47 Art 4 Z 4 DSG-VO.

48 Vgl Artikel 35 Abs 3 lit a DSG-VO zur Datenschutz-Folgenabschätzung.

49 Art 4 Z 2 DSG-VO: „Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

50 Dazu genauer *Ehrke-Rabel/Hödl*, DAKO 2017, 60.