# Recht der Digitalisierung II

Herausgegeben von
PHILIPP ANZENBERGER
und KLAUS SCHWAIGHOFER

*Internet und Gesellschaft*
*41*

**Mohr Siebeck**

Internet und Gesellschaft

Schriften des Alexander von Humboldt Institut
für Internet und Gesellschaft

Herausgegeben von

Jeanette Hofmann, Matthias C. Kettemann,
Björn Scheuermann, Thomas Schildhauer
und Wolfgang Schulz

41

# Recht der Digitalisierung II

## Internationalisierung der Justiz im digitalen Zeitalter

Herausgegeben von
Philipp Anzenberger und Klaus Schwaighofer

Mohr Siebeck

*Philipp Anzenberger*, geboren 1986, Studium der Rechtswissenschaften, sowie der Betriebswirtschaftslehre und Geographie (im Rahmen von Umweltsystemwissenschaften), 2014 Promotion zum Doktor der Rechtswissenschaften, 2019 Habilitation für die Fächer Zivilverfahrensrecht und Bürgerliches Recht, seit 2022 Universitätsprofessor am Institut für Zivilgerichtliches Verfahren der Leopold-Franzens-Universität Innsbruck.

*Klaus Schwaighofer*, geboren 1956, 1979 Promotion zum Doktor der Rechte, 1987 Habilitation für das Fach Strafrecht, Strafprozessrecht und Kriminologie, 1996 Ernennung zum Universitätsprofessor für Strafrecht, Strafprozessrecht und Kriminologie an der Leopold-Franzens-Universität Innsbruck, seit 1.10.2024 emeritiert.

ISBN 978-3-16-162589-3 / eISBN 978-3-16-162590-9
DOI 10.1628/978-3-16-162590-9

ISSN 2199-0344 / eISSN 2569-4081 (Internet und Gesellschaft)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind über *https://dnb.dnb.de* abrufbar.

Publiziert von Mohr Siebeck Tübingen 2025.

© Philipp Anzenberger, Klaus Schwaighofer (Hg.); Beiträge: jeweiliger Autor/jeweilige Autorin.

Dieses Werk ist lizenziert unter der Lizenz „Creative Commons Namensnennung – Weitergabe unter gleichen Bedingungen 4.0 International“ (CC BY-SA 4.0). Eine vollständige Version des Lizenztextes findet sich unter: https://creativecommons.org/licenses/by-sa/4.0/.

Jede Verwendung, die nicht von der oben genannten Lizenz umfasst ist, ist ohne Zustimmung der jeweiligen Urheber unzulässig und strafbar.

Gedruckt auf alterungsbeständiges Papier. Satz: Laupp & Göbel, Gomaringen.

Mohr Siebeck GmbH & Co. KG, Wilhelmstraße 18, 72074 Tübingen, Deutschland
www.mohrsiebeck.com, info@mohrsiebeck.com

# Vorwort der Herausgeber

Die Leopold-Franzens-Universität Innsbruck hat vor einigen Jahren beschlossen, einen Forschungsschwerpunkt im Bereich der Digitalisierung und Internationalisierung zu setzen. Zur Umsetzung dieses Schwerpunkts veranstaltet die Rechtswissenschaftliche Fakultät seit Sommersemester 2023 eine Ringvorlesung zu diesen Themen, wobei alternierend verschiedene Institute federführend sind. Zum Auftakt fand im März 2023 der vom Institut für Theorie und Zukunft des Rechts organisierte erste Digitalrechtstag statt. Die Vorträge auf dieser Tagung wurden im ersten Band „Recht der Digitalisierung: Herausforderungen der digitalen Governance in Wendezeiten" veröffentlicht.

Der nun vorliegende zweite Band enthält die Schriftfassungen aller Vorträge, die im Rahmen der Ringvorlesung im Wintersemester 2023/24 und im Sommersemester 2024 an der Universität Innsbruck gehalten wurden: Die Vorträge im Wintersemester 2023/24 wurden vom Institut für Strafrecht, Strafprozessrecht und Kriminologie organisiert und behandeln verschiedene Aspekte der Digitalisierung und Internationalisierung im Bereich des materiellen Strafrechts und Strafverfahrensrechts: *Severin Glaser* beschäftigt sich mit strafbaren Handlungen mit Kryptowährungen und unbaren Zahlungsmitteln, *Lorenzo Picotti* mit Künstlicher Intelligenz und Strafrecht, *Klaus Schwaighofer* mit dem Einsatz der Videotechnologie im Strafverfahren und deren Vereinbarkeit mit den Prozessgrundsätzen, *Andreas Venier* mit der Sicherstellung und Auswertung von Daten (insb. Smartphones), *Konrad Kmetic* mit dem Beitrag der Europäischen Staatsanwaltschaft zur grenzüberschreitenden Strafverfolgung und *Günther Hauss* mit der Europäischen Bankenaufsicht und Sanktionen gegen systemrelevante Banken in Europa.

Die Vorträge im Sommersemester 2024 waren thematisch der Digitalisierung und Internationalisierung im Zivil- und Zivilverfahrensrecht gewidmet und wurden vom den Instituten für Zivilrecht, Zivilgerichtliches Verfahren und Unternehmensrecht organisiert. Der Beitrag von *Philipp Anzenberger* beschäftigt sich mit Videoverhandlungen und Videobeweisaufnahmen im Zivilverfahren, jener von *Manfred Büchele* mit Fragen der Digitalisierung im Immaterialgüterrecht, *Amalia Diurni* untersucht das Thema „Human Vulnerability in Interaction with AI", *Bernhard Koch* stellt Neuerungen bei der Produkthaftung im digitalen Zeitalter vor, *Rupprecht Podzsun* und *Sarah Hinck* diskutieren die Macht in der digitalen Plattformökonomie, und *Stefano Troiano* und *Stefano Gatti* beschäftigen sich mit dem „right to data portability under the GDPR and beyond".

Einige dieser Vorträge wurden vom Institut für Italienisches Recht beigesteuert und sind in englischer Sprache verfasst, um sie der Leserin und dem Leser besser zugänglich zu machen. Wir hoffen, dadurch einen interessanten Querschnitt zu den Problemen und Fragen zu bieten, die die fortschreitende Digitalisierung und Internationalisierung in diesen Bereichen der Rechtswissenschaften aufwerfen.

Zu danken haben wir dem Dekan der Rechtswissenschaftlichen Fakultät der Universität Innsbruck, Herrn Univ.-Prof. Dr. *Walter Obwexer*, der für die Finanzierung dieses Bands gesorgt hat. Besonderer Dank gilt weiters Herrn Univ.-Ass. Mag. *Felix Rathgeb* für seinen Einsatz bei der Organisation und Erstellung des gesamten Tagungsbands sowie Frau Univ.-Ass. Mag.ª *Lena Gaggl*, Herrn Univ.-Ass. Mag. *Bernhard Hager*, Frau Univ.-Ass. Mag.ª *Maria Paulmichl* und Frau Stud.-Ass. *Leila Fasching*, die sich bei der Überarbeitung und Vereinheitlichung der Manuskripte verdient gemacht haben. Dem Verlag Mohr Siebeck und insbesondere Frau *Daniela Taudt-Wahl* und Frau *Silja Meister* möchten wir für die Drucklegung und die freundliche Betreuung danken.

Innsbruck, im Jänner 2025

*Philipp Anzenberger*
*Klaus Schwaighofer*

# Inhaltsverzeichnis

# Abkürzungsverzeichnis

| | |
|---|---|
| a. A. | andere Ansicht |
| a. a. O. | am angeführten Ort |
| a. M. | anderer Meinung |
| ABl. | Amtsblatt der Europäischen Union |
| ABoR | Administrative Board of Review |
| Abs. | Absatz |
| ACM | Autoriteit Consument en Markt |
| AGCM | Autorità garante della Concorrenza e del Mercato |
| AI | artificial intelligence |
| AIDP | Association Internationale de Droit Pénal |
| al. | alter |
| AMLA | Anti Money Laundering Authority |
| Anm. | Anmerkung |
| AnwBl | Anwaltsblatt |
| API | Application Programming Interface |
| arg. | argumentum |
| ARHG | Auslieferungs- und Rechtshilfegesetz |
| ARHV | Auslieferungs- und Rechtshilfeverordnung |
| Art. | Artikel/Article |
| Aufl. | Auflage |
| ausf. | ausführlich |
| AußStrG | Außerstreitgesetz |
| Az. | Aktenzeichen |
| BCBS | Basel Committee on Banking Supervision |
| BegrRegE | Begründung Regierungsentwurf |
| Beschl. | Beschluss |
| betrDEStA | betrauter Delegierter Europäischer Staatsanwalt |
| BGBl. | Bundesgesetzblatt |
| BGH | Bundesgerichtshof |
| BGHSt | Entscheidungen des Bundesgerichtshofs in Strafsachen |
| BiBuG | Bilanzbuchhaltungsgesetz |
| BIS | Bank for International Settlements |
| BKA | Bundeskanzleramt der Republik Österreich |
| BKartA | Bundeskartellamt |
| BlgNR | Beilagen zu den stenographischen Protokollen des Nationalrats |
| BMJ | Bundesministerium für Justiz |
| Bsp. | Beispiel |
| bspw. | beispielsweise |
| BT-Drs. | Drucksache Deutscher Bundestag |

| | |
|---|---|
| BudgetbegleitG | Budgetbegleitgesetz |
| BWG | Bankwesengesetz |
| bzw. | beziehungsweise |
| ca. | circa |
| CAC | Cyberspace Administration of China |
| CAs | conversational agents |
| CEBS | Committee of European Banking Supervisors |
| cf. | confer |
| COREPER | Ausschuss der Ständigen Vertreter |
| CRD | Capital Requirements Directive |
| CRR | Capital Requirements Regulation |
| DA | Data Act |
| DGA | Data Governance Act |
| Dir. | Directive |
| DMA | Digital Markets Act |
| DRiZ | Deutsche Richterzeitung |
| DRM | Digital Rights Management |
| DSA | Digital Services Act |
| DSG | Datenschutzgesetz |
| DS-GVO | Datenschutz-Grundverordnung |
| dZPO | deutsche Zivilprozessordnung |
| e. g. | exempli gratia |
| EBA | European Banking Authority |
| ebd. | ebenda |
| ECJ | European Court of Justice |
| ecolex | Zeitschrift für Wirtschaftsrecht |
| ed(s). | editor(s) |
| ed. | edition |
| EDIS | European Deposit Insurance Scheme |
| Edit. | Edition |
| EDPB | European Data Protection Board |
| EDPS | European Data Protection Supervisor |
| EEA | Europäische Ermittlungsanordnung |
| EG | Europäische Gemeinschaft |
| EGMR | Europäischer Gerichtshof für Menschenrechte |
| EHDS | European Health Data Space |
| EHR | electronic health records |
| Einl. | Einleitung |
| EIOPA | European Insurance and Occupational Pensions Authority |
| eJABl | Elektronisches Amtsblatt der österreichischen Justizverwaltung |
| EKHG | Eisenbahn- und Kraftfahrzeughaftpflichtgesetz |
| ELI | European Law Institute |
| EMRK | Europäische Menschenrechtskonvention |
| endg. | endgültig |
| Entsch. | Entscheidung(en) |
| Entw. | Entwurf |
| EO | Exekutionsordnung |
| ERA | Europäische Rechtsakademie |

| | |
|---|---|
| Erläut. | Erläuterungen |
| ErläutRV | Erläuterungen zur Regierungsvorlage |
| ErwGr. | Erwägungsgrund |
| ESFS | European System of Financial Supervision |
| ESMA | European Securities and Markets Authority |
| ESRB | European System Risk Board |
| EStG | Einkommensteuergesetz |
| et al. | et alter |
| etc. | et cetera |
| et seq. | et sequens |
| et seqq. | et sequentes |
| EU | Europäische Union |
| EuBagatellVO | Europäische Verordnung zur Einführung eines europäischen Verfahrens für geringfügige Forderungen |
| EuBVO | Europäische Beweisaufnahmeverordnung |
| EuDigiJustVO | Europäische Verordnung über die Digitalisierung der justiziellen Zusammenarbeit |
| EU-FinAnpG | EU-Finanz-Anpassungsgesetz |
| EuG | Gericht der Europäischen Union |
| EuGH | Europäischer Gerichtshof |
| EU-JZG | Bundesgesetz über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union |
| EU-RhÜbk | Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union |
| EUStA | Europäische Staatsanwaltschaft |
| EUStA-DG | Bundesgesetz zur Durchführung der Europäischen Staatsanwaltschaft |
| EUStA-VO | Verordnung zur Durchführung einer verstärkten Zusammenarbeit zur Errichtung der Europäischen Staatsanwaltschaft |
| EuZW | Europäische Zeitschrift für Wirtschaftsrecht |
| EvBl | Evidenzblatt der Rechtsmittelentscheidungen der ÖJZ |
| EZB | Europäische Zentralbank |
| f. | und der/die folgende |
| Fallnr. | Fallnummer |
| ff. | und der/die folgenden |
| FM-GwG | Finanzmarkt-Geldwäschegesetz |
| Fn. | Fußnote |
| fn. | footnote |
| FRIA | Fundamental Rights Impact Assessment |
| FSE | Fascicolo Sanitario Elettronico |
| FTC | Federal Trade Commission |
| G7 | Group of Seven |
| GAFAM | Google, Apple, Facebook, Amazon und Microsoft |
| GD GROW | Generaldirektion Binnenmarkt, Industrie, Unternehmertum und KMU |
| GD JUST | Generaldirektion Justiz und Verbraucher |
| GDPR | General Data Protection Regulation |
| gem. | gemäß |

| | |
|---|---|
| ggf. | gegebenenfalls |
| GOG | Gerichtsorganisationsgesetz |
| GP | Gesetzgebungsperiode |
| GRUR Int. | Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil |
| GWB | Gesetz gegen Wettbewerbsbeschränkungen |
| h. M. | herrschende Meinung |
| HBÜ | Haager Beweisaufnahme-Übereinkommen |
| HDAB | health data access body |
| HMI | human-machine interaction |
| i. d. F. | in der Fassung |
| i. d. R. | in der Regel |
| i. e. | id es |
| i. e. S. | im engeren Sinn |
| i. S. | im Sinn von |
| i. S. d. | im Sinn des/der |
| i. V. m. | in Verbindung mit |
| i. w. S. | im weiteren Sinn |
| IBOA | institutions, bodies, offices and agencies of the EU |
| iFamZ | Interdisziplinäre Zeitschrift für Familienrecht |
| IO | Insolvenzordnung |
| IoT | Internet of Things |
| IRP | Internal Rules of Procedure |
| Iss. | Issue |
| ITS | Implementing Technical Standards |
| JBl | Juristische Blätter |
| JCA | Journal of Consumer Affairs |
| JETL | Journal of European Tort Law |
| JN | Jurisdiktionsnorm |
| JSt | Journal für Strafrecht |
| JST | Joint Supervisory Teams |
| JuBG | Justiz-Begleitgesetz |
| JusIT | Zeitschrift für IT-Recht, Rechtsinformation und Datenschutz |
| Kap. | Kapitel |
| KI | Künstliche Intelligenz |
| KMU | kleine und mittlere Unternehmen |
| KVR | Rechtsbeschwerdeverfahren in Kartell-Verwaltungssachen |
| leg. cit. | legis citatae |
| Lfg. | Lieferung |
| lit. | litera |
| LK-StPO | Linzer Kommentar zur Strafprozessordnung |
| LLM | Large Language Model |
| LoseBl | Loseblattsammlung |
| LSI | less significant institutions |
| LUISS | Libera Università Internazionale degli Studi Sociali |
| m. a. W. | mit anderen Worten |
| m. E. | meines Erachtens |
| m. n. | marginal number |
| m. w. N. | mit weiteren Nachweisen |

| | |
|---|---|
| ME | Ministerialentwurf |
| MiCA | Markets in Crypto-Assets |
| Mio. | Millionen |
| MR | Medien und Recht |
| Mrd. | Milliarden |
| MR-Int | Medien und Recht International |
| NCA | national competent authorities |
| NJW | Neue Juristische Wochenschrift |
| NJW-Beil. | Neue Juristische Wochenschrift – Beilage |
| NLG | Natural Language Generation |
| no. | number |
| NPHRL | Entwurf einer neuen Produkthaftungsrichtlinie |
| Nr. | Nummer |
| NSCAI | National Security Commission on Artificial Intelligence |
| NTF | New Technologies Formation |
| NZKart | Neue Zeitschrift für Kartellrecht |
| ÖBl | Österreichische Blätter für Gewerblichen Rechtsschutz und Urheberrecht |
| ÖBl-LS | ÖBl-Leitsätze |
| ODR | Online Dispute Resolution |
| OECD | Organisation for Economic Co-operation and Development |
| OGH | Oberster Gerichtshof |
| ÖJA | Österreichisches Juristisches Archiv |
| OJEU | Official Journal of the European Union |
| öJGG | österreichisches Jugendgerichtsgesetz |
| ÖJZ | Österreichische Juristenzeitung |
| ÖJZ-MRK | Entscheidungen zur MRK in der ÖJZ |
| OLAF | Europäisches Amt für Betrugsbekämpfung |
| OLG | Oberlandesgericht |
| öStGB | österreichisches Strafgesetzbuch |
| öStPO | österreichische Strafprozessordnung |
| OTF | Organised Trading Facility |
| öUrhG | österreichisches Urheberrechtsgesetz |
| öZPO | österreichische Zivilprozessordnung |
| para. | paragraph |
| PHRL | Produkthaftungsrichtlinie |
| PIF-Richtlinie | Richtlinie über die strafrechtliche Bekämpfung von gegen die finanziellen Interessen der Union gerichtetem Betrug |
| PIMS | personal information management systems |
| PLF | Product Liability Formation |
| PSA | Payment Services Austria |
| RDi | Recht Digital |
| rec. | recital |
| RegE | Regierungsentwurf |
| RL | Richtlinie |
| Rn. | Randnummer |
| Rs. | Rechtssache |
| RtDP | right to data portability outlined by the GDPR |

| | |
|---|---|
| RTS | Regulatory Technical Standards |
| RZ | Österreichische Richterzeitung |
| S. | Satz |
| s. | siehe |
| s. o. | siehe oben |
| SARs | socially assistive robots |
| Sec. | Section |
| sent. | sentence |
| SI | significant intsitutions |
| SME | small and medium-sized enterprises |
| SRM | Single Resolution Mechanism |
| SSM | Single Supervisory Mechanism |
| SSRN | Social Science Research Network |
| SSt | Entscheidungen des Obersten Gerichtshofs in Strafsachen und Disziplinarangelegenheiten |
| StA | Staatsanwaltschaft |
| StPRÄG | Strafprozessrechtsänderungsgesetz |
| StrEU-AG | Strafrechtliches EU-Anpassungsgesetz |
| u. a. | unter anderen/anderem |
| US | United States |
| u. U. | unter Umständen |
| UAbs. | Unterabsatz |
| UK | United Kingdom |
| UNESCO | United Nations Educational, Scientific and Cultural Organization |
| untDEStA | unterstützender Delegierter Europäischer Staatsanwalt |
| Urt. | Urteil |
| usw. | und so weiter |
| v. | von/vom |
| v. a. | vor allem |
| Vers. | Version |
| vers. | version |
| VfGH | Verfassungsgerichtshof |
| VG | Verwaltungsgericht |
| vgl. | vergleiche |
| VLP | very large platforms |
| VO | Verordnung |
| Vol. | Volume |
| VPN | Virtual Private Network |
| vs. | versus |
| WK-StPO | Wiener Kommentar zur Strafprozessordnung |
| WP29 | Article 29 Working Group on Data Protection |
| WTBG | Wirtschaftstreuhandberufsgesetz |
| Z. | Ziffer |
| z.B. | zum Beispiel |
| Zak | Zivilrecht aktuell |
| ZEuP | Zeitschrift für Europäisches Privatrecht |
| ZFR | Zeitschrift für Finanzmarktrecht |

| | |
|---|---|
| ZfRV | Zeitschrift für Europarecht, internationales Privatrecht und Rechtsvergleichung |
| ZIK | Zeitschrift für Insolvenzrecht und Kreditschutz |
| ZPD | zentraler Plattformdienst |
| ZUM | Zeitschrift für Urheber- und Medienrecht |
| zust. | zustimmend |
| ZVN | Zivilverfahrens-Novelle |
| ZWF | Zeitschrift für Wirtschafts- und Finanzstrafrecht |

# Artificial Intelligence and Criminal Law

## Challenges to Some Traditional Categories

*Lorenzo Picotti*



## I. Introduction

The challenges that technological evolution has always posed to legal formants now find a new object in the emergence of artificial intelligence. The concept embraces a multiplicity of systems, operating in the digital sphere or even in the physical world, if equipped with hardware, such as robots or self-driving vehicles, in any case interacting with human beings and the environment. Besides immeasurable benefits for individuals and the community, however, they also create new risks, due to the decision-making autonomy that characterises them to varying degrees, based on autonomous learning mechanisms from the web and the external environment. Hence a diaphragm is interposed between the act of man 'behind' such machines and their behaviour or effects, which may be 'unpredictable' and offend legal goods, including fundamental rights, deserving criminal protection: Thus, the need to adapt the criteria for attributing liability to the natural and legal persons in whose interest they

operate, while at the same time respecting the guarantee principles of criminal law, in particular of legality and of culpability. In this regard, the recommendations on substantive criminal law that the *Association Internationale de Droit Pénal* approved in the international congress held in Paris in juin 2024, dedicated to the topic of criminal justice in the face of artificial intelligence, are taken into account.

## II. The Challenges of Technological Development to Legal Formants: The Emergence of Artificial Intelligence

The challenges of technological development to criminal law have always represented a stimulus to innovation in its three recognised formants.

First of all, they prompt legislators to critically examine existing legislation, in order to fill in any gaps with new provisions, to check if they are deemed necessary to deal with unlawful or socially harmful conduct that may be manifested through new technologies or to their detriment; gaps that the prohibition of analogy should prevent jurisprudence from overcoming by way of interpretation, in the daily endeavour to respond to new cases of offence (or new ways of offence) to traditionally protected legal goods, and sometimes also to new interests that have emerged as a result of technological developments.

No less stimulating is the need to verify, on a doctrinal level, the resilience of the dogmatic categories on which the attribution or modulation of criminal liability is based, in light of phenomena that may require their adaptation or even their partial overcoming, in favour of new attribution models. And in this regard, the dilemma may arise as to whether to renounce criminal protection, considering the content of traditional categories as an insurmountable limit of punitive intervention, with possible recourse to alternative techniques of protection (of a civil or administrative nature, for example), or whether one can or must review their conceptual content, without prejudice to their systematic function, within the limits in which they express principles of guarantee and of certainty that cannot be renounced.

For some time now, such demands have emerged in view of developments in the so-called risk society that characterises our age.[1] Consider, for instance, the environment, in its various articulations and components, facing the multiple phenomena of pollution and the risks of climate change; or the risks arising from defective products or from food and drink production techniques; or, again, the risks to the rights of the individual when confronted with developments in genetics and medicine, as well as

[1] On the wide-ranging debate that has developed internationally on the relationship between criminal law and the modern risk society, see the well-known contribution of *Prittwitz*, Strafrecht und Risiko. Untersuchungen zur Krise von Strafrecht und Kriminalpolitik in der Risikogesellschaft, 2nd ed., 2021; the careful remarks of *Sieber*, The Paradigm Shift in the Global Risk Society: From Criminal Law to Global Security Law – An Analysis of the Changing Limits of Crime Control, Journal of Eastern-European Criminal Law 2016, Iss. 1, 14.

to privacy and other rights, including those of a patrimonial nature, in the face of offences and threats originating from the spread of information and communication technologies, which has characterised the last half century at the turn of the new millennium.[2]

In this context, in which a strong drive has emerged in European and international law to adapt criminal protection, which has been deemed to be extended to respond to the new threats, a further challenge is now represented by the development of artificial intelligence (henceforth: AI), due to the very rapid spread of 'systems' that, even without our clear awareness, make use of AI, both in purely digital spheres (think of search engines, which are queried on a daily basis, or the 'personalised' online offer of films, music, travel, products, advertisements, social groups to join, etc.) and in the physical world, if equipped with hardware (so-called embedded AI), such as robots or other devices, like for example self-driving cars or so-called smart weapons.

The latest developments of the so-called generative AI, of which ChatGPT is the symbol, are having a strong impact, with great expectations in public opinion and in the market. ChatGPT is capable of producing and offering new contents 'created' autonomously in response to users' questions, with which it can establish a real dialogue, including a vocal one.

There is no denying the immeasurable advantages for individuals and the community to be derived from such developments, both economically and in terms of security and efficiency of disparate services and activities, given the great speed, precision, and capacity for action and reaction, based on the gathering and processing of enormous quantities of information, acquired in real time from the web and the outside world by means of optical, acoustic and thermal sensors, etc. As a result, AI systems can not only support, but also replace humans in an increasing number of functions and activities, especially if they are dangerous or complex, or even merely repetitive, being able to respond autonomously to external stresses, including adverse events, even accidental ones, or cyber or other attacks (think of military defence systems using so-called smart weapons).

However, new risks are also emerging, which need to be adequately addressed, linked precisely to the progressive replacement of man and, therefore, to the loss of his direct and complete control over the activities gradually 'delegated' to AI systems, which are entrusted with decisions and behaviours, even of vital importance. One may think of a road accident caused by or ascribable to the autonomous driving of a vehicle, or of a surgical operation performed by a specific robot with an adverse outcome; or (entering the field of malicious conduct) of stock exchange trading managed by means of so-called high-frequency algorithms, leading to market manipulation; or even of killings or injuries to persons carried out by means of drones or other

[2] For an up-to-date overview please refer to *Picotti*, Diritto penale, tecnologie informatiche ed intelligenza artificiale: una visione d'insieme, in: Cadoppi/Canestrari/Manna/Papa (eds.), Cybercrime, 2nd ed., 2023, 32 (35 et seq.).

so-called smart weapons, capable of autonomously identifying, selecting and hitting targets, without direct control or specific command by a human being, etc.

The need for protection in the face of these and similar risks and events cannot be distinguished from those for which the legal system already offers a criminal response. To a first approximation, therefore, it cannot be accepted that they go unpunished, because the use of an AI system is involved in their realisation; all the more since their progressive diffusion would widen the gaps in protection in the near future, creating a sort of immunity for the subjects (individuals and collective entities) who design, produce, distribute, use them, in their own interest or advantage.[3]

## III. On the Essential Characteristics of AI Systems and Possible Frictions with Certain Penal Categories

The technical peculiarities of artificial intelligence highlight, however, possible frictions with well-established categories of criminal law, such as causality and culpability, on which criminal responsibility is based.

Assuming that there is no unitary and recognised legal definition of artificial intelligence, to be considered as a metaphor evocative of a plurality of different techniques and systems,[4] two elements that characterise such systems appear which are very relevant to criminal law.

The first is that such AI systems are based on multiple and increasingly sophisticated (self-)learning techniques, called machine learning (such as those based on the so-called neural networks, capable of reproducing storage mechanisms analogous to those of the human mind), with which they autonomously acquire enormous quantities of data and information of all kinds, both in cyberspace (thanks to the growing availability of data, personal and otherwise, fed by the daily activities of billions of users and entities), and in the outside world, through the aforementioned optical, acoustic, thermal sensors, etc.

The speed and power of today's connections allow their immediate gathering, selection, processing, and sharing with other systems, in accordance with the purposes pursued: thus, the information 'material' on which they are based is not (only) that provided or chosen by the human being, but is sought and identified, and in part even created, without the human's intervention – in the case of generative AI – by the systems themselves.

Relevant is the 'training' that the systems develop using increasing amounts of data and information, in order to progressively reduce error margins. One may think

[3] On this subject, please see *Picotti*, The challenges of new technologies for European criminal law, in: Luchtman (ed.), Of swords and shields: due process and crime control in times of globalization. Liber Amicorum Prof. Dr. J. A. E. Vervaele, 2023, 805, and there further bibliographical indications.

[4] A reference could now be made to Art. 3 para. 1 of the AI Act.

of facial recognition techniques, but also of moving vehicles, or objects such as road signs or obstacles in traffic, which require comparison with the maximum possible amounts of images and sounds, reproducing different faces or things of similar categories, and their parts, in different contexts.

The second relevant aspect is that, alongside and in close correlation with this cognitive profile, there is a corresponding space of autonomy of decisions, even operational ones, that AI systems are able to take, minimising time and errors, compared to what a human agent or even an organised entity based on the activity of physical persons could do; decision-making autonomy that can also be expressed in the ability of the algorithms themselves to adapt, without specific human intervention, on the basis of the experience they have acquired, which thus makes their final behaviour or output 'unpredictable' (or not entirely predictable).

Because of these characteristics, a 'will' seems to emerge in the systems themselves, distinct from that of humans, which also differentiates AI systems from common computer systems, whose functioning is based on mathematical calculations according to predefined programmes, albeit complex, moving from a determined set of data, which have long been the subject and reason for reformatory interventions in criminal legislation at the supranational and national level.[5]

The action of AI systems now raises new issues, involving philosophy and ethics, which are committed to defining its characteristics and, if possible, orienting it, distinguishing actions of AI systems from man's acting and thinking, characterised by the 'conscience' of himself and his actions, which delineates his will as the expression of a freedom (more or less extensive) of self-determination in his relations with others and with society. And it is on this freedom that moral and social, even before legal, responsibility for its own actions is based, which would not be conceivable – at least at the current stage of technological development – for AI systems as such.

Their growing autonomy of decision and behaviour does, however, create a diaphragm, in terms of causation and culpable attribution, with respect to the human act, which remains at the origin of the design, production, finalisation, and use of these systems, in a chain that is so articulated and in many places obscure (one speaks of a black box, to designate the recurring situation in which it is not possible to retrace all the steps and modalities, often unrepeatable, through which an AI system arrives at a certain output), so as to make it problematic to ascribe the 'fact' realised to the human agent – natural person or entity – who is nevertheless 'behind the machine'.[6]

---

[5] For a recent overview on the implementation of the Cybercrime Convention, if desired, see again *Picotti*, I primi vent'anni della convenzione di Budapest nell'ottica sostanzialstica e la mancata ratifica ed esecuzione del primo protocollo addizionale contro il razzismo e la xenofobia, Diritto penale e processo 2022, Iss. 8, 1028 (1028 et seq.).

[6] For a careful analysis, based on broad international literature and attentive to the technological as well as the juridical profiles of the topic, see *Giannini*, Criminal Behavior and Accountability of Artificial Intelligence Systems, 2023.

## IV. The Recommendations of the *Association Internationale de Droit Pénal* Concerning Substantive Criminal Law

The *Association Internationale de Droit Pénal* (AIDP), at the end of its last five-year Congress held in Rome at the LUISS University in 2019, decided to devote the work of the XXI. congress, held in Paris in June 2024 – on the occasion of the centenary of its foundation, which took place just a century ago in the French capital – on the topic 'Artificial Intelligence and Criminal Justice' in its different aspects. In addition to those of substantive criminal law, to which the first two sections were dedicated, dealing respectively with the general and the special part, the criminal process was also strongly involved (to which the third section was dedicated), starting with the topic of the search and collection of evidence, by means of algorithms and intelligent agents, up to the scenarios of the so-called 'predictive' justice and policing, with all the advantages and risks of entrusting to such systems – increasingly relevant – parts of the functioning of criminal justice; while important reflections also concerned the international dimension, from judicial cooperation to humanitarian law, with particular attention to the use of smart weapons (Autonomous Weapon System), to which the fourth section was devoted.

In previous years, the work of the different sections has been carried out using the 'AIDP method', based on the collection of national reports, which respond to a questionnaire formulated by the *rapporteur général* of each section, who then draws up a general report and draws up a draft resolution that is then submitted to the representatives of the various national groups who participate in a specific international Colloquium, for each section, in which the text containing the 'recommendations' that AIDP addresses to legislators, magistrates, politicians, practitioners, citizens as well as criminal law scholars, is discussed, amended, supplemented and, finally, approved, in order to propose reasonable answers to the issues addressed.

To date, all four resolutions discussed at the International Colloquia in Syracuse (September 2022) for section I, in Bucharest (June 2023) for section II, in Buenos Aires (March 2023) for section III and, most recently, in Opatija (December 2023) for section IV have been approved and are or will be available on the AIDP website.[7]

### *1. Criminal Protection Requirements for Offensive Acts Carried out through or to the Detriment of AI Systems: The Man 'Behind' the Machine*

Only the profiles of substantive criminal law can be dealt with here, starting from the recommendations approved at the outcome of the work of section I on the topic: 'Traditional criminal law categories and AI: crisis or palingenesis?'[8], supplemented

[7] Available at https://www.penal.org/ (last accessed on: 7 July 2024).

[8] The general report edited by the undersigned, the adopted resolution, and a selection of country reports are published in Revue Internationale de Droit Pénal 2023, Iss. 1, 11, 53 and 93 et seqq. respectively.

by those approved at the outcome of the work of Section II, concerning the special part.[9]

Fundamental is the recognition that the development and dissemination of AI systems, certainly desirable because they represent a formidable advance for society as a whole, constitute at the same time a new source of risks, precisely because, as they become increasingly autonomous, their operation and their outcomes may, as has been said, be 'unpredictable' even for those who design, programme, produce, distribute and use them.

Moreover, they can play a growing and increasingly insidious role as a 'tool' for committing criminal acts, facilitated or directly carried out by AI systems, as in the case of smart weapons or high-frequency algorithms.

As the fields of application broaden, the illicit or harmful acts may harm a plurality of interests, legal goods and even fundamental rights, which require adequate protection, while respecting the fundamental principles of criminal law, starting with those of legality, offensiveness, proportionality and culpability.

But the traditional models of criminal liability must be reconsidered and adapted, if necessary, to respond effectively to emerging protection needs, as already indicated by numerous supranational sources, mostly of soft law.[10]

A special definition for criminal purposes of artificial intelligence, a notion that, moreover, does not find unambiguous answers even in the IT field, did not seem to be recommended.

Rather, it is preferable to consider the specific characteristics of the various AI systems, which have different degrees of autonomy, and the legal definitions that may be provided by non-criminal sources for specific sectors, such as that of self-driving vehicles.[11]

The usefulness and appropriateness of recognising AI systems – at least at the current stage of technological development – a legal subjectivity, or penal capacity, whereby they could be direct recipients of precepts and sanctions, has been unanimously ruled out, both on account of their ontological distinction from human agents and of the impossibility of pursuing punishment against them.

---

[9] The general report edited by *Prof. F. Miró-Llinares*, the resolution approved in Bucharest, and a selection of national reports are published in Revue Internationale de Droit Pénal 2024, Iss. 1.

[10] See the 'Ethical Guidelines for Trustworthy AI' presented to the European Commission on 8 April 2019 by the High Level Expert Group; the 'Feasibility Study on a future Council of Europe Instrument on Artificial Intelligence and Criminal Law' by the European Committee on Crime Problems from 4 September 2020, and especially the European Regulation on Artificial Intelligence (cf. so-called AI Act), 2024/1689 of 13 June 2024.

[11] Regarding the rules in force in France, Germany and, experimentally, Italy, it suffices to refer to the respective national reports published in the cited issue of the Revue Internationale de Droit Pénal: *Lacaze*, French Report on Traditional Criminal Law Categories and AI, Revue de Droit Pénal 2023, Iss. 1, 153; *Beck*, German Report on Traditional Criminal Law Categories and AI, Revue de Droit Pénal 2023, Iss. 1, 195, *Barresi*, Italian Report on Traditional Criminal Law Categories and AI, Revue de Droit Pénal 2023, Iss. 1, 269.

On the one hand, AI systems do not (as of yet) have a conscious freedom of choice and evaluation of possible solutions to a practical problem or dilemma, considering, with the necessary flexibility, also the context of social and ethical relations and opportunities in which they operate; on the other hand, the threat and application of sanctions, albeit *sui generis*, would be emptied of effect by the absence of self-awareness of their existence in the past, present and future: hence even excluding the retributive function, due to the lack of a corresponding ethical-moral perception, not even those of special prevention and general prevention would be usefully pursued.

Consequently, the need arises to create or adapt models for attributing criminal liability to the various human agents (both natural persons and entities) that 'stand behind' the machine, i. e. to the actors in the various phases of its life cycle: from designers, to manufacturers, sellers, owners, deployers and end users, who decide on its concrete use, according to their interest and benefit.

But first, or at least in parallel with reforms and interventions of a penal nature, it has been hoped that legislators – at the international, national and regional level – as well as the competent authorities, will fully define, according to their respective powers, the regulation of the various fields in which AI systems operate, as paradigmatically seen in France and Germany, with reference to the circulation of self-driving vehicles (see footnote 10).

In particular, the essential technical standards, structural characteristics and operating conditions that AI systems and their components must possess before being placed on the market or becoming operational, interacting with the environment and people, should be established, also by means of preventive authorisation and control systems.

This is a pre-condition, with respect to the intervention of criminal law, which must be able to punish offences attributable to the operation or 'behaviour' of AI systems in accordance with the principle of *ultima ratio*.

However, the need for reasonable and proportionate criminal protection has been reaffirmed on the basis of the criterion, referred to above, that if offences to interests, legal goods and fundamental rights caused by AI systems were committed (entirely) by natural or legal persons, they would constitute a crime, or at least a punishable offence: hence they cannot go unpunished for the fact that they are committed by, through or even against the said systems.

### *2. Criminal Liability for the Unlawful Use of AI Systems*

The approved resolution distinguishes between hypotheses in which AI systems are used in activities that are per se unlawful, and hypotheses in which they are used in activities that are per se lawful, but from which risks or offences may arise.

In the former case, the focus is mainly on intentional conduct, which poses fewer problems in terms of attributing criminal liability, since the use of AI systems to

commit an offence does not appear conceptually different from the use of other means to achieve a criminal end.

However, two specific recommendations have been made:

The first recommendation concerns cases where the results of the system's operation are deviant from the purpose pursued by the human agent. In such cases, the principles of *aberratio ictus* and *aberratio delicti* should be applied. The mere material diversity of the injured object, on the one hand, should not, in fact, be an excuse if its characteristics are not relevant to the legal case that configures the criminal offence (the killing of one person instead of another by an intelligent weapon is not relevant to the commission of the offence of intentional homicide, since it is in any case foreseen and intended by the agent).

In the case, on the other hand, of the commission of an offence other than the one intended (the injuring of persons, rather than the damaging of military facilities), criminal liability should be based on the 'possibility of foreseeing' the different development of the action brought about by the AI system, applying the principles of culpable liability, as specified, however, in the following part of the resolution.

The second recommendation, since AI systems can be used to carry out particularly damaging or dangerous acts, in which the offence is amplified and aggravated, compared with what human conduct could produce, with consequences that are also very distant from the actions from which they originate, it is recommended to consider incriminating, as autonomous preparatory offences, conduct referable to the design, production, sale, purchase stages, having as their object the development of algorithms, software and 'malicious' systems, intended solely or principally to commit offences.

This choice of criminal policy, in line with the perspective expressed in the aforementioned European regulation on artificial intelligence (AI-Act), should be limited to AI systems or their components, that present particularly high risks to very significant legal assets (such as life, physical safety, freedom of other human beings) and only in the event of a clear, real and present danger, in accordance with the recommendations approved in the context of Section I of the 18th AIDP Congress in Istanbul in 2009, concerning 'The extension of forms of preparation for and participation in crime'.[12]

### *3. Criminal Liability Arising from the Lawful Basic Use of AI Systems*

Instead, in cases where artificial intelligence systems are used in lawful basic activities, from which, moreover, relevant offences may result, the most delicate questions arise from a criminal law perspective.

---

[12] Cf. *Picotti*, L'élargissement des formes de préparation et de participation – Rapport général, Revue Internationale de Droit Pénal 2007, Iss. 3, 355; while the text of the resolution approved in Istanbul can be read in the same Revue: Revue Internationale de Droit Pénal 2015, Iss. 1, 421.

Firstly, it must be acknowledged that, even in this field, there cannot fail to be an area of 'permitted risk', ethically or in any case socially acceptable, the extent of which depends on the concrete balance between the benefits that the recourse to AI systems guarantees and the 'adverse events' that may ensue, the elimination of which cannot be possible in absolute terms, but the reduction or containment of which must be reasonably pursued in order to make them wholly exceptional, having regard to the importance of the legal assets at stake.

This area should be defined upstream, by means of the aforementioned extra-criminal regulation, from which specific security obligations and precautionary rules should flow, to be applied in advance, right from the mentioned activities of design, development, production, sale, as well as use of AI systems.

Secondly, the adjustment of criminal liability models must overcome the frictions between the assumptions and criteria for attributing fault, traditionally understood, and the technical characteristics of AI systems, characterised by decision-making autonomy, concrete unpredictability of behaviour, opacity of output production mechanisms, complexity of the programming, development, production, updating and maintenance process, in which different subjects intervene.

The reason for this is the gradualness of the levels of automation in the different areas in which they operate – from those in which operation is 'automated' for many functions, but still allows the human agent to have significant control over the overall 'behaviour' of the systems, to those in which they are truly 'autonomous', so that human intervention can only be at a distance, in time and space, from their immediate decision-making operations – the wide structural margin of 'unpredictability' of concrete outcomes must be compensated for by resorting to appropriate models of imputation to the human agents 'behind it'.

In this regard, the imputation of 'crime' liability of legal persons could constitute a first reference, alongside those of product liability and liability for the protection of health and safety in the workplace. In these areas, which are already legally regulated and harmonised also at a European level, innovative principles have emerged to ground the imputation by way of fault of offences resulting from complex chains of contributions, active and omissive, with respect to legal rules of conduct or technical standards to be complied with, referring to the various subjects participating in a single organisation or to interrelated entities and centres.

To summarise: a prior assessment of the risks inherent in the specific lawful, but also potentially dangerous, activities that are carried out by or through AI systems must be demanded, to be contained within the limits of the permitted risk, concretely defined by correlated obligations of prevention and caution concerning the specific sources of danger represented by the types of systems and activities that are from time to time at issue.

In this way, it is also possible to outline duties to prevent offences, especially in the event of red flags or previous adverse events, to be imposed on categories of persons

on the basis of their respective competences, which establish a position of guarantee on their part, also of criminal relevance.

### *4. On the Guarantee Positions and Guilt of Natural Persons*

On the basis of these assumptions, the AIDP recommendations distinguished in more detail the positions of natural persons from those of legal persons. For the former, the criminal charge must be based on the identification of the aforementioned positions of guarantee, in relation to the competences and functions performed, starting with that of the owner or apex representative of the organisation, who produces, manages, deploys or uses the AI system in his own interest or to his own advantage. Alongside top management positions, in complex organisations one must also consider intermediate positions and those responsible for corporate compliance, which presuppose an internal formalisation of positive obligations of a technical, organisational and control nature.

Liability for fault can thus comply with the general principles of criminal law, and in particular with the principle of personal culpability, since the objective link between the causal contribution of the human agent (possibly also by omission) and the commission of the offence is not sufficient, even if it can be traced, in its outcome, to the 'decisions' of the AI system. The foreseeability and avoidability of the unlawful act is in practice absorbed by the violation of the specific precautionary rules mentioned, established by sources, including secondary sources and internal provisions based on the preventive assessment of risks, and specifically aimed at containing them, without prejudice to the guiding criterion of 'not having acted differently' from what would have been possible and proper, which is the basis of the personalistic reproach.

In any event, actual foresight and awareness of the fact concretely realised by the AI system should not be required (there being no need for 'conscious negligence'). In fact, the object of the reproach may also be a fact that is simply ascribable to the type of event or conduct that should and could have been avoided by observing the required precautions, notwithstanding the subjective 'unforeseeability' of the concrete final damaging outcome (in the example of the investment of a pedestrian in particular light or traffic conditions, due to insufficient training of the autonomous guidance system, liability for fault on the part of the programmer and/or producer should not be excluded).[13]

This would not be a fault for not having foreseen the unforeseeable, as has been critically observed,[14] but rather for not having acted by preparing and adapting, according to the best science and technological experience in the sector, up-to-date

[13] Conversely, the liability of the user on board, who could not have detected the anomaly in the behaviour in time to intervene by switching to manual driving of the vehicle, should be excluded.

[14] *Piergallini*, Intelligenza artificiale: da 'mezzo' ad 'autore' del reato? Rivista italiana di diritto e procedura penale 2020, Vol. 63 Iss. 4, 1745 (1771).

measures for the containment and monitoring of the typical risk inherent in that activity, which were possible and necessary and would have ensured the performance of that activity within the limits of what was permitted.

### *5. Organisational Fault and Punitive Liability of Legal Persons*

Since a large proportion of AI systems are produced, distributed or used by companies, collective bodies and legal persons, the AIDP resolution recommends that they should also be subject to 'punitive' liability (not necessarily criminal liability in the strict sense) for acts constituting offences committed by, through or against AI systems.

Such liability should be based on the tried and tested model of 'organisational fault', to be recognised in the lack, deficiency or inadequacy of organisational and preventive measures, to be implemented and updated on the basis of the prior assessment of the specific risks arising from the activities entrusted to or, in any case, carried out by the AI systems, in the interest or to the advantage of the entity itself.

The principle of culpability would be respected, in that a requirement of individualised 'reproachability' of the entity must be demanded – at a subjective level – for not having acted differently from what it should have and could have done, to be added to the objective causal link between the activity carried out by the entity and the event or offence produced by the AI system, avoiding models of mere objective liability, albeit well-known and accepted in Anglo-Saxon systems.

Lastly, the body's liability should be autonomous and not depend on the criminal liability of a specific natural person in an apical or subordinate position with the body, since the latter should rather be held liable even if no natural person is individually punishable, because he is not identified or because of the particular conditions and circumstances that, in particular, characterise the chain upstream of the concrete operation of the AI system, to which the act is to be attributed (in assonance with the paradigmatic provision of Art. 8 of the Italian Legislative Decree 231/2001).

For this reason, it is recommended that in legal systems limiting the liability of entities to a closed list of offences (like the Italian one), it should be extended to include all offences that may be committed through, by or against AI systems.

### *6. Applicable Penalties*

As for the criminal penalties to be applied to natural persons, they should on the one hand also include imprisonment in proportion to the seriousness of the offences attributable to them.

On the other hand, pecuniary sanctions should be applicable to legal persons, possibly of an administrative nature, depending on the different legal systems, but in any event of a punitive nature, in addition to disqualification measures and suspension of the activity in the context of which the offence was committed. Other measures should include an injunction to change the compliance model and the possibility of a

public monitoring period to ensure that the AI system conforms to the imposed standards.

Given the potential seriousness of the damage that may result from the unlawful or harmful use of AI systems, it is also recommended that preventive measures be taken that immediately affect their use (such as seizure, judicial monitoring, or prohibitory measures applicable prior to conviction).

In any case, having to recognise the problematic nature of implementing within a reasonable timeframe an effective system of criminal or punitive liability for the natural and legal persons 'behind' the AI systems, the prompt adoption of complementary protection techniques appears to be recommended, which could range from the need for prior authorisation and administrative certification to civil law and insurance remedies.

Further alternatives to criminal prosecution and/or punitive response could include the dissemination of compliance models and restorative justice interventions.

### *7. The AIDP Recommendations on the Special Part*

Important findings also emerged in the recommendations concerning the special part, approved as a result of the work of section II and the related International Colloquium held in Bucharest in June 2023.

On the basis of the national reports and the general report edited by *Prof. Fernando Miró-Llinares* of the University of Elche, the need was considered to reform or adapt, if possible by way of interpretation, the existing criminal offences to ensure an adequate response to the new phenomena, which by their nature require a harmonised approach at supranational level.

Reaffirming that criminal law can only intervene as a last resort, the catalogue of the main offences that can be linked to the use of AI systems or perpetrated to their detriment was analysed.

It has thus emerged that a large proportion of the criminal offences related to AI systems can already be subsumed under existing incriminations, such as those punishing common offences of event (such as culpable homicide or culpable personal injury, in the case of injury to life or personal safety in the context of road traffic with autonomously driven vehicles, or of unfortunate or harmful outcomes of medical-surgical activities in which AI and robotic systems are used), or computer and cybercrimes, according to the provisions of the 2001 Council of Europe Cybercrime Convention (such as offences of unauthorised access to computer systems and damage to computer systems, even if only to software or data), since the general definition of 'computer system' may, without prejudice to their specific features, also include AI systems.

The same criterion applies to the dissemination of illicit content online, which may be produced and disseminated by means of AI systems, but may fall within the existing offences of child pornography or hate crimes or incitement to racial and other

discrimination, as well as the so-called deep fakes, capable of conditioning political and ideological orientations, detrimental to the proper functioning of the democratic system, especially electoral.

It was therefore recommended that if, on the one hand, the mere involvement of an AI system does not in itself justify new incriminations, nor an aggravation of the applicable penalties, on the other hand, it may be necessary to introduce new preparatory or purely dangerous offences, even beyond the general provision in Art. 6 of the Budapest Convention, where the existing offences are unable to guarantee adequate protection with respect to the greater seriousness or extension of the offences that may be irreparably determined by the application of AI systems, or to the rank of the legal goods at stake. It therefore seems consistent to introduce also autonomous cases of anticipation of criminal liability for the violation of specific rules of diligence, monitoring, and control by the various human agents involved in the chain of human conduct upstream, with respect to the operation, application, distribution and concrete use of AI systems, whose harmful effects can then be produced remotely.

In the catalogue of specific interests whose protection may merit criminalisation choices, the new ultra-individual dimension that privacy now acquires has been highlighted, attacked by the massive collection of personal data aimed not only at profiling, advertising, and 'personalised' propaganda through AI systems, but also to systematically carry out crimes against property, such as credit card fraud and online payment means.

And even sophisticated techniques of image or information manipulation, on which decision-making procedures are based in various public and private venues, which can lead to discrimination or serious violations of dignity and personality, might deserve specific intervention by criminal law, on a par with those that can distort or divert the responses of the most modern so-called generative AI systems.

## V. Concluding Remarks

To sum up, the overwhelming technological evolution we are witnessing and the usefulness and, at the same time, risks we are experiencing, and have to acquire full awareness, in order to make the best use of it, cannot be a sphere extraneous to criminal law in its various forms.

As jurists, we need to be confronted without delay with these developments, which have an increasing impact on the whole spectrum of criminal justice, including trial, international cooperation, and humanitarian law. And even the theory of crime is called upon to rethink itself, starting from the basic concept of 'conduct' or, better, the criminally relevant 'action', which is the cornerstone of the offence, but can no longer be said to be only 'human', even if the classical physical-naturalistic concept of bodily movement has been overcome, because even the finalistic and personalistic concept is undermined by the overbearing contribution of AI systems, which once in

the field 'decide' autonomously, precisely in the last essential link of the fact itself, being able to deviate from the subjectively pursued or at least 'foreseeable' outcomes.

The effects of the algorithms' activities, however, do not remain closed within technological apparatuses or in cyberspace, but redound in social relations. Therefore, one cannot accept the expansion of a space that is free from law, or even only from criminal law, by renouncing an effective protection of legal goods, which under the current legal system deserve such strong protection.

The answer can only be that of 'accountability', including criminal accountability of the persons and human entities that 'stand behind' the intelligent machines by means of appropriate charging models that, while innovating, where necessary, the content of the traditional dogmatic categories, nevertheless respect the superordinate principles of guarantee, in particular of legality, offensiveness, proportionality and culpability.

# Digitalisierung im materiellen Strafrecht

## Strafbare Handlungen mit Kryptowährungen und unbaren Zahlungsmitteln

*Severin Glaser*



Kryptowerte stellen mittlerweile einen bedeutsamen Bestandteil des Wirtschaftslebens in Österreich, Europa und der ganzen Welt dar. Dies hängt zweifellos mit einer stets steigenden Aufgeschlossenheit gegenüber neuen Technologien auch im sensiblen Bereich der Zahlungsvorgänge zusammen, die sich außerdem in ähnlicher Weise bei der zunehmend selbstverständlichen Verwendung von Internetbanking oder kontaktlosen Zahlungssystemen zeigt. Der vorliegende Beitrag beleuchtet einige grundsätzliche materiell-rechtliche Problemstellungen, die sich im Zusammenhang mit Kryptowerten und unbaren Zahlungsmitteln *de lege lata* ergeben. Dabei wird das Hauptaugenmerk auf die Schwierigkeiten im Hinblick auf die relevanten Begriffsbestimmungen und die daraus resultierenden Folgewirkungen gelegt. Hingewiesen wird darüber hinaus auf strafanwendungsrechtliche Probleme im Kontext mit Kryptowährungen und unbaren Zahlungsmitteln.

## I. Begriff der Kryptowährung, der virtuellen Währung und des Kryptowerts

Der Begriff der Kryptowährung ist dem Strafrecht fremd; nicht so jedoch die Begriffe der virtuellen Währung und des Kryptowerts. Das öStGB verwendet den Begriff der virtuellen Währung an einer einzigen Stelle, nämlich in § 165 Abs. 6 öStGB. In

dieser Bestimmung wird klargestellt, dass virtuelle Währungen eine Teilmenge des Begriffs „Vermögensbestandteile“ sind, der dem Tatobjekt der Geldwäscherei zugrunde liegt. Eine Definition des Begriffs der virtuellen Währung enthält das öStGB allerdings weder an dieser noch an anderer Stelle, ebenso wenig wie die europarechtlichen Vorgaben zur Kriminalisierung der Geldwäscherei, insbesondere die RL 2018/1673.[1] Es findet sich jedoch folgende Legaldefinition für den Begriff der virtuellen Währung in der zentralen europarechtlichen Vorgabe zur Geldwäscheprävention, der 4. Geldwäsche-RL[2] i. d. F. 5. Geldwäsche-RL[3] (Art. 3 Z. 18) und gleichlautend in der strafrechtsrelevanten RL 2019/713[4] (Art. 2 lit. d):

„eine digitale Darstellung eines Werts, die von keiner Zentralbank oder öffentlichen Stelle emittiert wurde oder garantiert wird und nicht zwangsläufig an eine gesetzlich festgelegte Währung angebunden ist, die nicht den rechtlichen Status einer Währung oder von Geld besitzt, aber von natürlichen oder juristischen Personen als Tauschmittel akzeptiert wird und die auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann“.

Diese Begriffsbestimmung hat auch gleichlautenden Eingang in das österreichische Recht gefunden, und zwar in drei bundesgesetzliche Bestimmungen zur Geldwäscheprävention (§ 2 Z. 21 FM-GwG, § 87 Abs. 2 Z. 19 WTBG und § 43 Abs. 2 Z. 19 BiBuG). Darüber hinaus enthält § 27b Abs. 4 EStG für das Einkommensteuerrecht eine gleichlautende Legaldefinition für den Begriff der Kryptowährung.

Der zentrale Schwachpunkt dieser Begriffsbestimmung, der sich auch in der in Umsetzung der RL 2019/713 ergangenen, neuen Legaldefinition für unbare Zahlungsmittel in § 74 Abs. 1 Z. 10 öStGB findet, ist die explizite Ausklammerung gesetzlicher Zahlungsmittel. Der Begriff der gesetzlichen Zahlungsmittel stellt nicht etwa nur auf inländische Gesetze oder europarechtliche Normen ab, sondern beruht – wie generell der Begriff des Geldes – auf einem weltweiten Verständnis: Nicht nur das Falschmünzereiabkommen,[5] dem Österreich seit mehr als 90 Jahren angehört,[6] sondern auch die Straftatbestände des 23. Abschnitts des Besonderen Teils des

[1] Richtlinie (EU) 2018/1673 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 über die strafrechtliche Bekämpfung der Geldwäsche, ABl. L 284/22 vom 12.11.2018.

[2] Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission, ABl. L 141/73 vom 5.6.2015.

[3] Richtlinie (EU) 2018/843 des Europäischen Parlaments und des Rates vom 30. Mai 2018 zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU, ABl. L 156/43 vom 19.6.2018.

[4] Richtlinie (EU) 2019/713 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln und zur Ersetzung des Rahmenbeschlusses 2001/413/JI des Rates, ABl. L 123/18 vom 10.5.2019.

[5] International Convention for the Suppression of Counterfeiting Currency, Genf am 20.4.1929, LGTS, Vol. 45, 371.

[6] BGBl. 347/1931.

öStGB gehen – wie ausdrücklich in § 241 öStGB zu lesen – von einem Geldbegriff aus, der bewusst auch ausländische Währungen mitumfasst. Man stellt insoweit also auf die Eigenschaft als gesetzliches Zahlungsmittel in allen Rechtsordnungen der Welt ab, macht also die Reichweite des Rechtsbegriffs von Fremdrecht abhängig. In der vorliegenden Form eines Negativkriteriums führt diese – hier ohne erkennbare Notwendigkeit eingeführte – Fremdrechtsakzessorietät allerdings dazu, dass die wirtschaftlich wichtigste virtuelle Währung, der Bitcoin, rechtlich gesehen keine virtuelle Währung i. S. d. Art. 2 lit. d RL 2019/713, § 2 Z. 21 FM-GwG, § 87 Abs. 2 Z. 19 WTBG, § 43 Abs. 2 Z. 19 BiBuG, keine Kryptowährung i. S. d. § 27b Abs. 4 EStG und auch kein unbares Zahlungsmittel i. S. d. § 74 Abs. 1 Z. 10 öStGB ist, weil er den gesetzlichen Status einer Währung in El Salvador[7] besitzt.[8] Dieses Ergebnis ist kriminalpolitisch zweifellos unpraktikabel und geradezu ärgerlich, darf aber – zumindest im Strafrecht – ebenso zweifellos nicht durch eine Analogie bzw. teleologische Reduktion zulasten des Täters „korrigiert" werden.

Der Gesetzgeber könnte auch anders. Dies zeigt sich an der in der MiCA-VO[9] enthaltenen Legaldefinition für den Begriff Kryptowert (Art. 3 Abs. 1 Z. 5):

„eine digitale Darstellung eines Werts oder eines Rechts, der bzw. das unter Verwendung der Distributed-Ledger-Technologie oder einer ähnlichen Technologie elektronisch übertragen und gespeichert werden kann".

Diese u. a. für den Bereich des Marktmissbrauchs relevante Definition, auf die auch die 3. Geldtransfer-VO[10] (Art. 3 Z. 14) sowie der Vorschlag für die zukünftige Geldwäsche-VO[11] (Art. 2 Z. 13) verweisen, zeichnet sich gegenüber der zuvor dargestellten Begriffsbestimmung dadurch aus, dass er ausschließlich auf technische Eigenschaften abstellt und gesetzliche Zahlungsmittel nicht ausschließt;[12] der Bitcoin ist

---

[7] *Ley Bitcoin*, *Decreto 57*, *Diario Oficial*, San Salvador am 9.6.2021; die Zentralafrikanische Republik, die als weltweit zweiter Staat den Bitcoin zum gesetzlichen Zahlungsmittel erklärt hatte, hat diese Entscheidung im April 2023 wieder revidiert.

[8] *Glaser*, Der Bitcoin als staatliche Währung, ZWF 2021, 264 (265 f.); bezogen auf unbare Zahlungsmittel a. M. *Bauer-Raschhofer*, Die modifizierte Bekämpfung von Betrug und Fälschung bei unbaren Zahlungsmitteln, ZWF 2022, 50 (53); *Kattavenos-Lukan*, Das unkörperliche unbare Zahlungsmittel gem § 74 Abs 1 Z 10 StGB, ÖJA 2023, 107 (124); *Schroll/Oberressl*, in: Höpfel/Ratz (Hrsg.), Wiener Kommentar zum Strafgesetzbuch, 2. Aufl., 2024, § 74 StGB Rn. 60/38; *Bertel/Schwaighofer*, Österreichisches Strafrecht. Besonderer Teil II, 15. Aufl., 2022, § 241a StGB Rn. 3.

[9] Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über Märkte für Kryptowerte und zur Änderung der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 1095/2010 sowie der Richtlinien 2013/36/EU und (EU) 2019/1937, ABl. L 150/40 vom 9.6.2023.

[10] Richtlinie (EU) 2023/1113 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über die Übermittlung von Angaben bei Geldtransfers und Transfers bestimmter Kryptowerte und zur Änderung der Richtlinie (EU) 2015/849 (Neufassung), ABl. L 150/1 vom 9.6.2023.

[11] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung, Brüssel, den 20.7.2021, COM(2021) 420 final.

[12] ErwGr. 13 MiCA-VO stellt klar, wo der Anwendungsbereich der VO enden soll: „Digitale Vermögenswerte, die von Zentralbanken in deren Eigenschaft als Währungsbehörde ausgegeben werden, einschließlich Zentralbankgeld in digitaler Form, oder Kryptowerte, die von anderen Be-

somit ein Kryptowert im rechtlichen Sinne. Im Übrigen enthält die Legaldefinition des Kryptowerts auch kein wirtschaftliches Kriterium: Da es also auch nicht auf die Akzeptanz der Wertdarstellung als Tauschmittel ankommt, kommen auch (bloße) Anlageprodukte wie etwa *non-fungible tokens* im Bereich digitaler Kunstwerke als Kryptowerte in Betracht.

## II. Auswirkungen der (fehlenden) Legaldefinitionen für „Kryptowährung", „virtuelle Währung" und „Kryptowert"

Für den Begriff der Kryptowährung besteht derzeit nur im Einkommensteuerrecht eine Legaldefinition, nicht jedoch im Strafrecht. Dies bleibt freilich ohne Auswirkungen, solange das Strafrecht keine Rechtsfolgen an diesen Begriff anknüpft (ihm also insbesondere in Straftatbeständen keine Rolle zukommt). Die Nichtanwendbarkeit des einkommensteuerrechtlichen Begriffs der Kryptowährung auf gesetzliche Zahlungsmittel und somit auf den Bitcoin hat abgabenrechtliche Bedeutung, darüber hinaus aber allenfalls mittelbare Auswirkungen auf das Finanzstrafrecht, soweit das Vorliegen von Einkünften aus Kryptowährungen (§ 27b EStG) die Voraussetzung eines darauf bezogenen Verkürzungsdelikts (z. B. einer Abgabenhinterziehung) ist. Der Umstand, dass die außerstrafrechtlichen Legaldefinitionen für virtuelle Währungen im FM-GwG, WTBG und BiBuG ebenfalls auf gesetzliche Zahlungsmittel und damit auch auf Bitcoins nicht anwendbar sind, wirkt sich zwar auf den Bereich der Geldwäscheprävention (insbesondere die Meldepflichten und Risikoanalysen) aus, muss darüber hinaus aber keine materiell-rechtliche Auswirkung auf das Strafrecht haben: Obwohl das öStGB den Begriff der virtuellen Währung, den es nur an einer Stelle, beim Geldwäschereistraftatbestand, verwendet, selbst nicht definiert, ist eine Übernahme der unpraktikablen Begriffsbestimmung aus dem FM-GwG, dem WTBG und dem BiBuG m. E. nicht geboten.

Deutlich gelungener definiert ist hingegen der Begriff der Kryptowerte, der im Bereich des verwaltungsstrafrechtlichen Marktmissbrauchsrechts durch die MiCA-VO unmittelbare Geltung erfährt, und nach der bis 30.6.2024 bestehenden Möglichkeit gemäß Art. 111 Abs. 1 und Abs. 2 MiCA-VO auch das Tatobjekt gerichtlicher Marktmissbrauchstatbestände hätte bilden können. Da auch die Geldwäsche-VO auf diesen Begriff verweist, wird dadurch das Problem der Ausklammerung gesetzlicher Zahlungsmittel und damit auch des Bitcoins im zukünftigen Geldwäschepräventionsrecht behoben. Ein Verweis auf eine gleichlautende Legaldefinition wäre auch

---

hörden einschließlich zentraler, regionaler und lokaler Verwaltungsbehörden ausgegeben werden, sollten dem Unionsrahmen für Märkte für Kryptowerte nicht unterliegen." Diese Einschränkung würde den Bitcoin, der zwar gesetzliches Zahlungsmittel ist, aber weder von Zentralbanken noch anderen Behörden ausgegeben wird, nicht aus dem Begriff des Kryptowerts i. S. d. Art. 3 Abs. 1 Z. 5 MiCA-VO ausschließen.

in § 165 Abs. 6 öStGB anstelle der Verwendung des bisher undefinierten Begriffs der virtuellen Währung m. E. vernünftig.

## III. Begriff des unbaren Zahlungsmittels

Der Begriff des unbaren Zahlungsmittels findet Verwendung in den Straftatbeständen nach §§ 241a–241c, 241e–241f und 241h öStGB sowie in den Betrugsqualifikationen nach § 147 Abs. 1 Z. 1 2. Fall und 3. Fall öStGB („Zahlungsmittelbetrug", „Betrug mit ausgespähten Daten eines unbaren Zahlungsmittels"). Seit der Einführung des Begriffs im öStGB[13] bestand auch eine entsprechende Legaldefinition in § 74 Abs. 1 Z. 10 öStGB. Bis zu ihrer umfassenden Novellierung durch BGBl. I 201/2021 erfasste diese Legaldefinition „jedes personengebundene oder übertragbare körperliche Zahlungsmittel, das den Aussteller erkennen lässt, durch Codierung, Ausgestaltung oder Unterschrift gegen Fälschung oder missbräuchliche Verwendung geschützt ist und im Rechtsverkehr bargeldvertretende Funktion hat oder der Ausgabe von Bargeld dient". Es bestand nach dieser früheren Rechtslage Klarheit darüber, welche Produkte unter den Begriff des unbaren Zahlungsmittels fallen, nämlich die Bank-, Bankomat- und Kreditkarte, der Wechsel und der Scheck.

In Umsetzung der RL 2019/713 brachte BGBl. I 201/2021 eine Neufassung der Legaldefinition des § 74 Abs. 1 Z. 10 öStGB für unbare Zahlungsmittel als „nichtkörperliche oder körperliche Vorrichtungen, Gegenstände oder Aufzeichnungen oder deren Kombination, ausgenommen gesetzliche Zahlungsmittel, die vor Fälschung oder missbräuchlicher Verwendung geschützt sind und die für sich oder in Verbindung mit einem oder mehreren Verfahren dem Inhaber oder Nutzer ermöglichen, Geld oder monetäre Werte zu übertragen, auch mittels digitaler Tauschmittel". Die Neufassung unterscheidet sich von der bisherigen Definition durch die Aufgabe des Körperlichkeitserfordernisses; gerade im Bereich der Nichtkörperlichkeit zeigt sich jedoch die Nachteiligkeit der – bereits oben dargestellten – expliziten Ausnahme für gesetzliche Zahlungsmittel, die sich auch in der Legaldefinition für unbare Zahlungsmittel findet und wie schon ausgeführt auch insoweit zum Ausschluss des Bitcoins führt. Die positiven Erfordernisse eines unbaren Zahlungsmittels nach § 74 Abs. 1 Z. 10 öStGB sind also erstens das Vorliegen von Vorrichtungen, Gegenständen, Aufzeichnungen oder deren Kombination, zweitens ein Fälschungs- oder Missbrauchsschutz und drittens eine bestimmte Funktion, nämlich die Ermöglichung der Übertragung von Geld oder monetärer Werte (einschließlich digitaler Tauschmittel), und zwar entweder für sich oder in Verbindung mit einem oder mehreren Verfahren.

Die Verwendung einiger Begrifflichkeiten erklärt sich mit ähnlichen Terminologien in der europarechtlichen Vorgabe. So definiert Art. 2 lit. a RL 2019/713 den Begriff „unbares Zahlungsinstrument" als „nichtkörperliche oder körperliche ge-

[13] BGBl. I 15/2004.

schützte Vorrichtungen, geschützte Gegenstände oder geschützte Aufzeichnungen oder deren Kombination, ausgenommen gesetzliche Zahlungsmittel, die beziehungsweise der für sich oder in Verbindung mit einem oder mehreren Verfahren dem Inhaber oder Nutzer ermöglicht, Geld oder monetäre Werte zu übertragen, auch mittels digitaler Tauschmittel". Für Teilbegriffe dieser Begriffsbestimmung liegen ebenfalls Legaldefinitionen vor, die für das Verständnis der österreichischen Rechtsbegriffe bedeutsam sind. So definiert Art. 2 lit. b RL 2019/713 die „geschützte Vorrichtung, [den] geschützte[n] Gegenstand oder [die] geschützte Aufzeichnung" als „eine Vorrichtung, einen Gegenstand oder eine Aufzeichnung, die beziehungsweise der vor Fälschung oder betrügerischer Verwendung geschützt ist, z. B. durch das Design, eine Kodierung oder eine Unterschrift". Ein „digitales Tauschmittel" umfasst nach Art. 2 lit. c RL 2019/713 einerseits E-Geld i. S. d. RL 2009/110/EG[14] (also z. B. *paysafecards*[15]) und andererseits virtuelle Währungen.

Dennoch bleiben viele Begrifflichkeiten der Legaldefinition des § 74 Abs. 1 Z. 10 öStGB undeutlich, so etwa was genau unter einer Vorrichtung, einer Aufzeichnung oder einem Gegenstand – namentlich einem nichtkörperlichen – zu verstehen ist, und wann eine Kombination vorliegen könnte. Es liegt nahe, die schon früher unter den Begriff der unbaren Zahlungsmittel fallenden Bank-, Bankomat- und Kreditkarten, Wechsel und Schecks auch weiterhin als erfasst zu betrachten.[16] Aber auch ein Smartphone ist ein gegen Missbrauch geschützter Gegenstand, der bisweilen zur Übertragung von Geld genutzt wird, und könnte also bei Bestehen entsprechender Apps durchaus auch vom Wortlaut des Begriffs des unbaren Zahlungsmittels erfasst sein. Die ErläutRV nennen auch „Online-Banking" und „intermediäre Zahlungsabwickler" (z. B. PayPal oder Klarna[17]) als unkörperliche unbare Zahlungsmittel,[18] was wohl am ehesten einer Kombination aus nichtkörperlicher Vorrichtung (Zahlungssoftware) und nichtkörperlichen Aufzeichnungen (Zugangsdaten) entspricht.[19] Un-

---

[14] Art. 2 Z. 2 Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates vom 16. September 2009 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, zur Änderung der Richtlinien 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 2000/46/EG, ABl. L 267/7 vom 10.10.2009, definiert als E-Geld „jeden elektronisch – darunter auch magnetisch – gespeicherten monetären Wert in Form einer Forderung gegenüber dem Emittenten, der gegen Zahlung eines Geldbetrags ausgestellt wird, um damit Zahlungsvorgänge im Sinne des Artikels 4 Nummer 5 der Richtlinie 2007/64/EG durchzuführen, und der auch von anderen natürlichen oder juristischen Personen als dem E-Geld-Emittenten angenommen wird".

[15] *McAllister*, in: Wess (Hrsg.), Wirtschaftsstrafrecht, 2. Aufl., 2023, § 147 StGB Rn. 14; a. M. *Bauer-Raschhofer*, ZWF 2022, 50 (53); *Kattavenos-Lukan*, ÖJA 2023, 107 (123).

[16] Wohl in diesem Sinne zu verstehen ErläutRV 1099 BlgNR 27. GP 1; *Schroll/Oberressl*, in: Höpfel/Ratz, WK-StGB, 2. Aufl., 2024, § 74 StGB Rn. 60/4, 60/9, wobei die Autoren offenlassen, ob es sich insoweit um Vorrichtungen oder Gegenstände handelt.

[17] *BMJ*, Erlass vom 13. Dezember 2021 über die Regelungen des Bundesgesetzes, mit dem das Strafgesetzbuch und das Zahlungsdienstegesetz 2018 zur Umsetzung der Richtlinie zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln geändert werden, 2021-0.856.819, eJABl 30/2021, 3.

[18] ErläutRV 1099 BlgNR 27. GP 2.

[19] *Kattavenos-Lukan*, ÖJA 2023, 107 (113).

klar bleibt auch, warum die neue Legaldefinition die Art des geforderten Schutzes vor Fälschung oder missbräuchlicher Verwendung im Gegensatz zur früheren Legaldefinition nicht (mehr) präzisiert; würde wirklich jedes Hindernis gegenüber Fälschung oder missbräuchlicher Verwendung genügen, käme auch eine versperrbare Geldkassette als Missbrauchsschutz oder sogar selbst als unbares Zahlungsmittel in Betracht.[20] Schließlich wirkt auch die Funktion der Ermöglichung der Übertragung von Geld oder monetärer Werte dem Gesetzeswortlaut nach denkbar weit,[21] wenngleich sich aus den Erwägungsgründen der RL 2019/713 ergibt, dass ein unbares Zahlungsmittel nur bei Instrumenten mit Zahlungsfunktion vorliegen soll.[22]

## IV. Auswirkungen der Legaldefinition für „unbare Zahlungsmittel"

Konsequenz des Ausschlusses gesetzlicher Zahlungsmittel und des damit einhergehenden – in der Literatur teilweise in Abrede gestellten[23] – derzeitigen Ausschlusses des Bitcoins aus dem Begriff der unbaren Zahlungsmittel führt dazu, dass der Bitcoin derzeit auch weder Tatobjekt der Straftatbestände nach §§ 241a–241c, 241e–241f öStGB bzw. Bezugspunkt des Tatobjekts nach § 241h öStGB sein kann, noch als Tatmittel bzw. Bezugspunkt des Tatmittels der Betrugsqualifikationen nach § 147 Abs. 1 Z. 1 2. Fall und 3. Fall öStGB fungieren kann.

Die Existenz nichtkörperlicher unbarer Zahlungsmittel stellt eine neue Herausforderung für die Auslegung bestimmter Tatbestandsmerkmale der Zahlungsmitteldelikte bzw. Betrugsqualifikationen dar. Dazu zählen nicht nur einzelne Tathandlungen,[24] sondern noch viel grundsätzlicher die Tatobjekte: So beziehen sich die §§ 241a–241c öStGB sowie § 147 Abs. 1 Z. 1 2. Fall öStGB auf falsche oder verfälschte unbare Zahlungsmittel, wobei „falsch" und „verfälscht" bislang so wie bei Urkunden in §§ 223–224a, 226 und 147 Abs. 1 Z. 1 1. Fall öStGB im Hinblick auf Ausstellerauthentizität verstanden wurde: Falsch ist demnach ein unbares Zahlungsmittel, wenn der Anschein erweckt wird, das unbare Zahlungsmittel stamme von

---

[20] Vgl. die Stellungnahme von *Schmoller* (Stellungnahme zum ME einer StGB-Novelle 2021: unbare Zahlungsmittel, 5/SN-137/ME, 3), der sich dafür aussprach, die Wendung „durch Codierung, Ausgestaltung oder Unterschrift" auch in den neuen Wortlaut mitaufzunehmen.

[21] *Bauer-Raschhofer*, ZWF 2022, 50 (51).

[22] Vgl. ErwGr. 9 RL 2019/713. *Schroll/Oberressl*, in: Höpfel/Ratz, WK-StGB, 2. Aufl., 2024, § 74 StGB Rn. 60/4, 60/10 setzen diese Funktion mit der vor der durch BGBl. I 201/2021 herbeigeführten Neufassung der Legaldefinition geforderten bargeldvertretenden oder bargeldverschaffenden Funktion gleich.

[23] *Bauer-Raschhofer*, ZWF 2022, 50 (53); *Kattavenos-Lukan*, ÖJA 2023, 107 (124); *Schroll/Oberressl*, in: Höpfel/Ratz, WK-StGB, 2. Aufl., 2024, § 74 StGB Rn. 60/38.

[24] So geht *Unger* (Novellierung des StGB im Dunstkreis der Delikte bezüglich unbarer Zahlungsmittel, JusIT 2022, 9 [12]) davon aus, dass die in § 241b Abs. 1 öStGB genannten Tathandlungen des Einführens und Ausführens nur in Bezug auf körperliche unbare Zahlungsmittel begangen werden könnten, während umgekehrt die Tathandlung des Bereitstellens nur in Bezug auf nichtkörperliche unbare Zahlungsmittel begangen werden könnte.

einem anderen Aussteller, als es tatsächlich der Fall ist;[25] verfälscht ist es, wenn die Informationen eines echten unbaren Zahlungsmittels nachträglich unbefugt (verwechslungstauglich) geändert werden.[26] Diese Auslegung passt jedoch kaum zu unbaren Zahlungsmitteln, die anders als Bankomatkarten nicht mehr mit Urkunden vergleichbar sind, m. a. W. keine Gewährschaftsträger darstellen, was insbesondere bei nichtkörperlichen unbaren Zahlungsmitteln wie virtuellen Währungen der Fall ist.[27] Für diesen Umstand bestehen drei Lösungsmöglichkeiten: Zum ersten kann man das bisherige Verständnis von „falsch" und „verfälscht" beibehalten, kommt damit jedoch zur weitgehenden Unanwendbarkeit der genannten Tatbestände auf die neu hinzugekommenen (insbesondere die nichtkörperlichen) unbaren Zahlungsmittel.[28] Zweitens wäre es indessen auch möglich, innerhalb der genannten Straftatbestände zwischen körperlichen und nichtkörperlichen unbaren Zahlungsmitteln zu unterscheiden und je nach dem betroffenen unbaren Zahlungsmittel zu einem heterogenen Verständnis der Begriffe „falsch" und „verfälscht" zu kommen, wie es in ähnlicher Weise bereits jetzt innerhalb des § 147 Abs. 1 Z. 1 öStGB ein heterogenes Verständnis des Begriffs „falsch" gibt, je nachdem ob es um die Benützung eines Beweismittels oder eines anderen Tatmittels geht. Schließlich bestünde als dritte (aufwendigste) Variante die Möglichkeit, das bisherige Verständnis von „falsch" und „verfälscht" in den genannten Tatbeständen auch im Hinblick auf schon früher erfasste unbare Zahlungsmittel zugunsten eines neuen Begriffsverständnisses aufzugeben.

In ganz ähnlicher Weise stellt sich die Frage, wie bei der Auslegung des Begriffs „entfremdet" vorzugehen ist, soweit die Straftatbestände nach §§ 241e–241g öStGB bzw. die Betrugsqualifikation nach § 147 Abs. 1 Z. 1 2. Fall öStGB Bezug auf entfremdete unbare Zahlungsmittel nehmen. Bislang wurde der Begriff des Entfremdens in einem rein körperlichen Sinn (etwa als Gewahrsamsbruch) verstanden, nun existieren jedoch auch nichtkörperliche unbare Zahlungsmittel. Auch insoweit bestehen die Möglichkeiten der Nichtanwendung der Tatbestände bzw. Betrugsqualifikation auf nichtkörperliche unbare Zahlungsmittel, der völligen Aufgabe des bisherigen Verständnisses des Begriffs des Entfremdens zugunsten eines neuen Verständ-

---

[25] *Hinterhofer/Rosbaud*, Strafrecht Besonderer Teil II, 6. Aufl., 2016, § 241a StGB Rn. 13; *Kirchbacher/Sadoghi*, in: Höpfel/Ratz, WK-StGB, 2. Aufl., 2024, § 147 StGB Rn. 28/6; *Kert*, in: Hinterhofer (Hrsg.), Salzburger Kommentar zum Strafgesetzbuch, 41. Lfg., Dezember 2019, § 147 StGB Rn. 75; *Flora*, in: Leukauf/Steininger (Hrsg.), Strafgesetzbuch Kommentar, 4. Aufl., 2020, § 147 StGB Rn. 14b.

[26] *Hinterhofer/Rosbaud*, Strafrecht BT II, 6. Aufl., § 241a StGB Rn. 16; *Kirchbacher/Sadoghi*, in: Höpfel/Ratz, WK-StGB, 2. Aufl., 2024, § 147 StGB Rn. 28/8; *Kert*, in: Hinterhofer, SbgK-StGB § 147 StGB Rn. 78.

[27] *Schroll/Oberressl*, in: Höpfel/Ratz, WK-StGB, 2. Aufl., 2024, § 74 StGB Rn. 60/6.

[28] In diesem Sinne *Schroll/Oberressl*, in: Höpfel/Ratz, WK-StGB, 2. Aufl., 2024, § 74 StGB Rn. 60/6.

nisses, oder ein heterogenes Begriffsverständnis in Bezug auf körperliche und nichtkörperliche unbare Zahlungsmittel.[29]

## V. Strafanwendungsrechtliche Probleme

Im Hinblick auf nichtkörperliche unbare Zahlungsmittel ergeben sich nun auch verstärkte Tatbegehungsmöglichkeiten über das Internet, die in dieser Weise bei rein körperlichen Tatobjekten zuvor kaum vorstellbar gewesen wären. So wäre es etwa möglich, die Online-Banking-Webseite eines inländischen Opfers vom Ausland aus zu fälschen (und damit allenfalls den Tatbestand des § 241a Abs. 1 öStGB zu begehen) oder eine Online-Banking-Webseite eines inländischen Opfers vom Ausland aus unzugänglich zu machen (und damit allenfalls den Tatbestand des § 241e Abs. 3 öStGB zu begehen). Zusätzlich zu allen mit dem Tatbestand selbst verknüpften Problemen ergeben sich insoweit auch strafanwendungsrechtliche Fragestellungen. Diese resultieren hier – so wie bei allen Delikten, die über das Internet begangen werden – aus der Schwierigkeit, einen inländischen Tatort festzumachen, dem jedoch zur Anwendung der österreichischen Strafgesetze unter dem Territorialitätsprinzip (§ 62 öStGB) maßgebliche Bedeutung zukommt. Im Unterschied zu anderen Delikten, die – v. a. auf Basis des § 64 öStGB – ungeachtet des Rechts des Tatortstaates auch als Auslandstaten den österreichischen Strafgesetzen unterliegen können, beruht bei den Zahlungsmitteldelikten die Anwendbarkeit des österreichischen Strafrechts (neben den selteneren Fällen der §§ 63, 65 öStGB) auf dem Territorialitätsprinzip, setzt also einen Tatort im Inland voraus.

Die Einheitstheorie des § 67 Abs. 2 öStGB erkennt den Handlungsort des Täters ebenso wie den Erfolgsort gleichermaßen als Tatort an. Eine Straftat ist demnach an jedem Ort begangen, an dem der Täter gehandelt hat oder handeln hätte sollen (Versuch, Unterlassung) bzw. an dem ein tatbildmäßiger Erfolg ganz eingetreten ist, zum Teil eingetreten ist (wobei ein Zwischenerfolg, z. B. der themengleiche Irrtum beim Betrug, genügt[30]) oder nach der Vorstellung des Täters eintreten hätte sollen (Versuch). Hierbei ist festzuhalten, dass nur Erfolgsdelikte einen Erfolgsort haben, da § 67 Abs. 2 öStGB ausdrücklich auf den tatbildmäßigen Erfolg abstellt.[31] Im Unter-

---

[29] In letzterem Sinne *Salimi*, Die neue Richtlinie über unbare Zahlungsmittel und ihre Umsetzung in Österreich, in: Lewisch (Hrsg.), Jahrbuch Wirtschaftsstrafrecht und Organverantwortlichkeit 2022, 2022, 141 (145 f.); *Kattavenos-Lukan*, ÖJA 2023, 107 (111); *Bertel/Schwaighofer*, BT II, § 241e StGB Rn. 3; im Ergebnis wohl auch *Ley/Bichler*, Novellierung der Definition unbarer Zahlungsmittel und die Auswirkungen auf virtuelle Währungen, JSt 2022, 365 (366).

[30] Der Zwischenerfolg wird aber nur insoweit einen Erfolgsort als Tatort bilden können, als er selbst Teil des Tatbildes ist, *Jansen*, Die Inlandstat, 2014, 108 f., 111, 144, 176.

[31] In Österreich wird – einhellig – „ein dem Tatbild entsprechender Erfolg" i. S. d. Erfolgs der Erfolgsdelikte verstanden, vgl. *Triffterer*, in: Hinterhofer, SbgK-StGB, 4. Lfg., Mai 1996, § 67 StGB Rn. 14; *Schwaighofer*, in: Hinterhofer, SbgK-StGB, 44. Lfg., März 2023, § 62 StGB Rn. 24; *Salimi*, in: Höpfel/Ratz, WK-StGB, 2. Aufl., 2024, § 67 StGB Rn. 29, 78; *Glaser*, Strafanwendungsrecht in

schied dazu kann sich der Tatort bei schlichten Tätigkeitsdelikten nur aus dem Handlungsort ergeben.

Dies bedeutet für das Erfolgsdelikt des Betrugs einschließlich seiner Qualifikationen, also auch für den Zahlungsmittelbetrug und den Betrug mit ausgespähten Daten eines unbaren Zahlungsmittels, dass es einen Erfolgsort gibt, und es für die Begründung eines inländischen Tatorts und der Geltung der österreichischen Strafgesetze für die Tat genügt, dass das Opfer im Inland getäuscht wurde oder der Vermögensschaden in Österreich eingetreten ist.

Die Zuordnung der Zahlungsmitteldelikte zu den Erfolgs- oder schlichten Tätigkeitsdelikten ist nicht einheitlich. Die Fälschung unbarer Zahlungsmittel (§ 241a öStGB) stellt nach h. M. ein schlichtes Tätigkeitsdelikt dar,[32] und auch die Delikte nach §§ 241b und 241f öStGB dürften zur Gänze oder zumindest größtenteils als schlichte Tätigkeitsdelikte zu werten sein, allenfalls mit Ausnahme bestimmter Tatbegehungsalternativen wie dem Verschaffen eines falschen oder verfälschten unbaren Zahlungsmittels. Die Entfremdung unbarer Zahlungsmittel nach § 241e Abs. 1 und 3 öStGB dürfte hingegen ein Erfolgsdelikt sein und somit auch durch den Ort des jeweiligen Erfolgseintritts einen Tatort begründen.

## VI. Schlussfolgerungen

Die vorstehenden Ausführungen zeigen zunächst einige Schwierigkeiten, die mit der Definition bzw. fehlenden Definition der Begriffe „Kryptowährung“ und „virtuelle Währung“ im Strafrecht verbunden sind. Der derzeitige Ausschluss des Bitcoins aus den außerstrafrechtlichen Legaldefinitionen für virtuelle Währungen bzw. Kryptowährungen machen diese für eine Übernahme ins Strafrecht unpraktikabel. Insgesamt bleibt das Fehlen einer passenden Definition im Strafrecht derzeit noch ohne Folgen, und zwar auch bei der Geldwäscherei, wo der Begriff der virtuellen Währungen (undefiniert) Verwendung findet, wenngleich nur als Teilmenge des viel breiteren Begriffs der Vermögensbestandteile. Eine praktikablere Definition bietet die MiCA-VO für den Begriff der Kryptowerte, der durch das bloße Abstellen auf technische

---

Österreich und Europa, 2018, 170; OGH 12.3.1981, 12 Os 11/81 SSt 52/13 = ZfRV 1982, 48; OGH 16.5.2013, 13 Os 4/13g EvBl 2013/107; in Deutschland wird hingegen vertreten, dass „der zum Tatbestand gehörende Erfolg“ gemäß der Tatortdefinition des § 9 Abs. 1 dStGB nicht gleichbedeutend mit dem Erfolg eines Erfolgsdelikts sei, vgl. *Werle/Jeßberger*, in: Cirener/Radtke/Rissing-van Saan/Rönnau/Schluckebier (Hrsg.), Strafgesetzbuch Leipziger Kommentar, 13. Aufl., 2020, § 9 StGB Rn. 33; *Jäger*, in: Wolter (Hrsg.), Systematischer Kommentar zum Strafgesetzbuch I, 9. Aufl., 2017, § 9 StGB Rn. 7; BGH, Urt. v. 12.12.2000 – 1 StR 184/00 BGHSt 46, 212 = NJW 2001, 624 (*Toeben*) – Rn. 54.

[32] *Oshidari*, in: Hinterhofer, SbgK-StGB, 16. Lfg., April 2007, § 241a StGB Rn. 3; *Schroll*, in: Höpfel/Ratz, WK-StGB, 2. Aufl., 2024, § 241a StGB Rn. 1; a. M. *Kienapfel/Schmoller*, Strafrecht. Besonderer Teil III, 2. Aufl., 2009, § 241a StGB Rn. 3, die § 241a öStGB als Erfolgsdelikt erachten.

Erfordernisse jedenfalls auch den Bitcoin miteinschließt, und in Zukunft auch weit über den Bereich des Marktmissbrauchs einsetzbar wäre.

Auch die neu gefasste Begriffsbestimmung für unbare Zahlungsmittel in § 74 Abs. 1 Z. 10 öStGB klammert gesetzliche Zahlungsmittel (und damit derzeit den Bitcoin) aus und enthält auch darüber hinaus einige rätselhafte Elemente, die insbesondere mit der Aufgabe des bisher unabdingbaren Körperlichkeitserfordernisses zusammenhängen. Dies verursacht nicht nur eine Unklarheit über die Reichweite des Begriffs der unbaren Zahlungsmittel selbst, sondern auch über die Auslegung bestimmter Tatbestandsmerkmale in den mit unbaren Zahlungsmitteln in Verbindung stehenden Delikten, die wie etwa „falsch", „verfälscht" oder „entfremdet" in einem auf Körperlichkeit bezogenen Kontext verstanden wurden. Darüber hinaus ergeben sich gerade im Hinblick auf nichtkörperliche unbare Zahlungsmittel neue Begehungsformen für Delikte im Internet, die insoweit auch strafanwendungsrechtliche Probleme aufwerfen können, soweit die Zahlungsmitteldelikte schlichte Tätigkeitsdelikte darstellen.

# Digitalisierung im Strafverfahren

## Der Einsatz der Videotechnologie im Strafverfahren und deren Vereinbarkeit mit den Prozessgrundsätzen

*Klaus Schwaighofer*



## I. Einleitung

Der *Unmittelbarkeitsgrundsatz* galt und gilt als eine der wichtigsten Prozessmaximen im Strafverfahren. Personen, die irgendwelche Wahrnehmungen zu einem strafrechtlich relevanten Verhalten gemacht haben, sollen *in der Hauptverhandlung* möglichst *persönlich* erscheinen und ihre Zeugenaussage vor Gericht und den Parteien ablegen,

weil nur dieser unmittelbare Eindruck eine bestmögliche Würdigung von Aussagen und Feststellung des wahren Sachverhalts ermöglicht (sogenannte formelle Unmittelbarkeit).[1] Durch die Befragung durch den Vorsitzenden selbst und die Parteien kann sich das erkennende Gericht einen eigenen Eindruck vom verbalen und nonverbalen Aussageverhalten der Beweisperson machen.[2] Die Unmittelbarkeitsmaxime steht auch in enger Beziehung zur Aufklärungspflicht der Gerichte: Die zur Belastung und zur Verteidigung des Beschuldigten dienenden Umstände sind von Amts wegen bestmöglich mit der gleichen Sorgfalt zu ermitteln (§ 2 Abs. 2, § 3 Abs. 1 öStPO).[3] Und die Unmittelbarkeit des Verfahrens vermittelt der Öffentlichkeit auch ein besseres Bild von der Tätigkeit der Strafjustiz und ist insofern vertrauensbildend.

In Österreich bringt *§ 13 Abs. 3 öStPO* den *Vorrang des unmittelbaren Personalbeweises* deutlich zum Ausdruck: „Soweit ein Beweis unmittelbar aufgenommen werden kann, darf er nicht durch einen mittelbaren ersetzt werden."[4] Diese Bestimmung, auch materielle Unmittelbarkeit bezeichnet, wird durch *§ 252 öStPO* ergänzt, wonach Protokolle über die Vernehmung von Mitbeschuldigten und Zeugen, Vermerke, in denen Aussagen festgehalten worden sind, sowie Ton- und Bildaufnahmen über die Vernehmung bei sonstiger Nichtigkeit nur in bestimmten, in den Ziffern 1 bis 4 aufgezählten Ausnahmefällen verlesen oder vorgeführt werden dürfen.[5]

Auf Surrogate wie Protokolle oder auch Videoaufzeichnungen darf also nur ausnahmsweise, etwa zur Verhinderung von Beweisverlusten, im Interesse des Zeugenschutzes, aber auch aus prozessökonomischen Gründen (bei Zustimmung der Parteien) zurückgegriffen werden.[6] Nach der Konzeption der öStPO soll die *Hauptverhandlung* den *Schwerpunkt des Verfahrens* bilden (§ 13 Abs. 1 öStPO): Beweise sind in der Hauptverhandlung aufzunehmen und der maßgebliche Sachverhalt soll dort festgestellt werden. Die Hauptverhandlung soll mehr sein als eine bloße Überprüfung der Ergebnisse des Ermittlungsverfahrens,[7] es sei denn, die Sache ist unstreitig,

---

[1] *Birklbauer*, in: Birklbauer/Haumer/Nimmervoll/Wess (Hrsg.), StPO. Linzer Kommentar zur Strafprozessordnung, 2020, § 13 StPO Rn. 4; *Schmoller*, in: Fuchs/Ratz (Hrsg.), Wiener Kommentar zur Strafprozessordnung, 173. Lfg., Mai 2012, § 13 StPO Rn. 5; *Hinterhofer/Oshidari*, System des österreichischen Strafverfahrens, 2017, Rn. 2.193; *Kroschl*, in: Schmölzer/Mühlbacher (Hrsg.), StPO Strafprozessordnung I, 2. Aufl., 2021, § 13 StPO Rn. 3; siehe jüngst auch *Divjak*, Die grenzüberschreitende Videovernehmung im Strafverfahren, JSt 2024, 319 (328).

[2] *Hinterhofer/Oshidari*, System, Rn. 2.192; *Schmoller*, in: Fuchs/Ratz, WK-StPO § 13 StPO Rn. 7.

[3] *Bertel*, in: Bertel/Venier (Hrsg.), StPO-Kommentar I, 2. Aufl., 2022, § 13 StPO Rn. 2; *Jahn/Schmitt-Leonardy*, Unumstößliches Unmittelbarkeitsprinzip im Strafprozess? NJW 2022, 2721 (2722).

[4] Siehe auch *Schmoller*, in: Fuchs/Ratz, WK-StPO § 13 StPO Rn. 3, 34.

[5] *Fabrizy/Kirchbacher*, StPO und wichtige Nebengesetze, 14. Aufl., 2020, § 252 StPO Rn. 1; *Kirchbacher*, in: Fuchs/Ratz, WK-StPO, 354. Lfg., Dezember 2021, § 252 StPO Rn. 2 f., 10, 21; *Schmoller*, in: Fuchs/Ratz, WK-StPO § 13 StPO Rn. 5, 50; *Venier/Tipold*, Strafprozessrecht, 15. Aufl., 2022, Rn. 324.

[6] *Kirchbacher*, in: Fuchs/Ratz, WK-StPO § 252 StPO Rn. 22, 24; *Dangl/Schröder*, in: Birklbauer/Haumer/Nimmervoll/Wess, LK-StPO, 2020, § 252 StPO Rn. 4.

[7] *Schmoller*, in: Fuchs/Ratz, WK-StPO § 13 StPO Rn. 3; *Fabrizy/Kirchbacher*, StPO, 14. Aufl., § 13 StPO Rn. 1; *Kroschl*, in: Schmölzer/Mühlbacher, StPO I, 2. Aufl., 2021, § 13 StPO Rn. 1.

wenn z. B. ein Geständnis vorliegt, das durch objektive Beweisergebnisse gut abgesichert ist. In einem solchen Fall kann man auf die nochmalige unmittelbare Vernehmung von Zeugen aus verfahrensökonomischen Gründen verzichten.

Die Unmittelbarkeit lässt sich freilich nicht voll durchhalten. Manchmal bleibt im Interesse der Wahrheitserforschung nichts anderes übrig, als auf mittelbare Beweissurrogate zurückzugreifen, nach dem Motto „besser als gar nichts".[8] Aber es gibt auch zunehmend Überlegungen und Diskussionen, ob man von diesem eindeutigen *Vorrang der Unmittelbarkeit abrücken* sollte.[9] Die *Vorführung von Bild-Ton-Aufzeichnungen* von Vernehmungen im Ermittlungsverfahren sowie *audiovisuelle Vernehmungen* von Personen, die sich an einem anderen Ort befinden, sind denkbare Alternativen zur persönlichen, unmittelbaren Vernehmung in der Hauptverhandlung:

- Sie können zur *Beschleunigung* des Verfahrens beitragen und *Kosten sparen,* z. B. weil Reisekosten für Zeugen wegfallen oder ein verhafteter Angeklagter nicht vorgeführt werden muss.
- Sie können dem *Opferschutz* dienen, weil dem Opfer eine belastende zusätzliche Befragung über Details der Straftat in der Hauptverhandlung (und eine damit womöglich verbundene „sekundäre Viktimisierung") erspart wird, wenn bloß die Bild-Ton-Aufzeichnung der früheren Vernehmung in der Hauptverhandlung vorgeführt wird.
- Die Videoaufzeichnung einer frühen, tatnahen Vernehmung eines Zeugen könnte wegen der frischeren Erinnerung u. U. das *„bessere" Beweismittel* sein als die unmittelbare Vernehmung dieses Zeugen in der wesentlich später stattfindenden Hauptverhandlung.[10]
- Und in Zeiten der Corona-Pandemie kann auch der *Schutz vor Infektionen* ins Treffen geführt werden.

Es gibt also durchaus *Argumente,* die *für* eine Aufweichung des Unmittelbarkeitsgrundsatzes sprechen. Dem stehen freilich gewichtige *rechtsstaatliche Bedenken* gegenüber, weil Verteidigungsrechte des Beschuldigten dadurch eingeschränkt werden: Zu den essenziellen *Verteidigungsrechten* der EMRK (Art. 6 Abs. 3 lit. d EMRK), die in Österreich im Verfassungsrang steht, gehört das Recht des Angeklagten, Fragen an die Belastungszeugen zu stellen, häufig auch Konfrontationsrecht genannt. Dieses Recht kann optimal nur ausgeübt werden, wenn der Zeuge in der Hauptverhandlung persönlich anwesend ist und dort befragt werden kann.[11]

---

[8] *Schmoller*, in: Fuchs/Ratz, WK-StPO § 13 StPO Rn. 9.

[9] Unter anderem ist *Güntge* für eine Abschaffung des Unmittelbarkeitsgrundsatzes in seiner jetzigen Form, siehe *Güntge*, in: Thesen der Gutachterinnen und Gutachter sowie der Referentinnen und Referenten, 73. Deutscher Juristentag, Bonn 2022, abrufbar unter https://djt.de/wp-content/uploads/2022/08/220805_djt_73_thesen.pdf (Abrufdatum: 28.8.2024), 21 (21).

[10] *Güntge*, in: Thesen, 21.

[11] *Grabenwarter/Frank*, B-VG. Bundes-Verfassungsgesetz und Grundrechte, 2020, Art. 6 EMRK Rn. 32; *Hinterhofer/Oshidari*, System, Rn. 4.17.

Ich möchte zunächst einen Überblick über den Anwendungsbereich der Videotechnologie in der geltenden öStPO geben, das Spannungsverhältnis zu den Prozessgrundsätzen aufzeigen und schließlich daraus meine Schlussfolgerungen ziehen, ob bzw. in welchen Bereichen die Videotechnologie im Strafverfahren ausgebaut werden könnte und sollte.

## II. Der derzeitige Anwendungsbereich der Videotechnologie im österreichischen Strafverfahren

Die öStPO in der geltenden Fassung spricht an mehreren Stellen von der „Verwendung technischer Einrichtungen zur Wort- und Bildübertragung" bei Vernehmungen.[12] In der Regel ist damit die *audiovisuelle Übertragung* einer Vernehmung gemeint, bei der sich die Vernehmungsperson und die vernommene Person an verschiedenen Orten befinden. Es geht aber auch um die *Video-Aufzeichnung* von Vernehmungen, um sie später – in der Hauptverhandlung – verwenden zu können: sei es, dass die vernommene Person zu diesem Zeitpunkt nicht mehr verfügbar ist, weil sie nicht zur Hauptverhandlung kommen kann oder will, sei es, um der Beweisperson bei abweichenden Aussagen in der Hauptverhandlung die frühere Aussage vorhalten zu können oder zu überprüfen, ob das Protokoll, das bei jeder Vernehmung angefertigt wird, die Aussage zutreffend wiedergibt.

Die *Anfertigung einer Ton- und Bildaufnahme* der Vernehmung ist seit kurzem auch im *öJGG* vorgesehen, wenn ein Jugendlicher vernommen wird und weder ein Verteidiger noch eine Vertrauensperson anwesend ist (§ 36a Abs. 2, § 37 öJGG).

*Live-Übertragungen* von Gerichtsverhandlungen sind in Österreich – zu Recht – ausnahmslos verboten (§ 228 Abs. 4 öStPO, § 22 MedienG).[13]

### *1. Vernehmung von Zeugen im Ermittlungsverfahren, die sich in einem anderen Sprengel aufhalten (§ 153 Abs. 4 öStPO)*

Der im Jahr 2010 eingefügte § 153 Abs. 4 öStPO erlaubt die Vernehmung von Zeugen und Beschuldigten „unter Verwendung technischer Einrichtungen zur Wort- und Bildübertragung", wenn der *Aufenthaltsort eines Zeugen oder Beschuldigten außerhalb des Sprengels der zuständigen Staatsanwaltschaft oder des zuständigen Gerichts* gelegen ist. Sofern jedoch die unmittelbare Vernehmung unter Berücksichtigung der Verfahrensökonomie zweckmäßiger oder aus besonderen Gründen erforderlich ist,

[12] Siehe auch §§ 56a und 56b FinStrG, auf die in den folgenden Ausführungen aber nicht näher eingegangen wird.

[13] Siehe dazu zuletzt *Eckstein*, Gerichtsöffentlichkeit im digitalen Zeitalter, juridikum 2022, 440.

ist der Zeuge oder Beschuldigte dennoch vor die zuständige Staatsanwaltschaft oder vor das zuständige Gericht zu laden.[14]

Im Sinne der *Verfahrensökonomie* wird die Ladung und persönliche Vernehmung freilich kaum je zweckmäßiger sein, weil die Videovernehmung i. d. R. durch Zeit- und Kostenersparnis ökonomischer ist. Im Sinne der Wahrheitsfindung und Aufklärung wird hingegen der unmittelbaren Vernehmung i. d. R. der Vorzug zu geben sein.

### *2. Pflichtverhör zur Prüfung der Voraussetzungen der U-Haft (§ 172 Abs. 1 öStPO, § 174 Abs. 1 öStPO)*

Jeder Festgenommene ist grundsätzlich innerhalb von 48 Stunden ab Festnahme in die Justizanstalt des zuständigen Gerichts einzuliefern, oder, wenn der Festnahmeort entsprechend weit vom zuständigen Gericht entfernt ist, in die Justizanstalt eines unzuständigen Gerichts. Das Gericht muss die eingelieferte Person vernehmen und längstens binnen 48 Stunden nach der Einlieferung entscheiden, ob sie freigelassen wird oder ob die Untersuchungshaft verhängt wird (§ 174 Abs. 1 letzter Satz öStPO). Weil das bei *Einlieferung in ein unzuständiges Gericht* schwierig zu bewerkstelligen ist, erlaubt *§ 172 Abs. 1 öStPO* in diesem Fall, die Vernehmung des Beschuldigten unter Verwendung technischer Einrichtungen zur Wort- und Bildübertragung vorzunehmen und den Beschluss über die Untersuchungshaft auch auf diese Weise zu verkünden.[15]

Diese Bestimmung wurde anlässlich der Corona-Pandemie im Jahr 2020 ergänzt[16] und *§ 153 Abs. 4 öStPO generell* für das sogenannte *Pflichtverhör* vor der Entscheidung über die Untersuchungshaft für anwendbar erklärt (§ 174 Abs. 1 öStPO).[17] Festgenommene Beschuldigte konnten also vom Haft- und Rechtsschutzrichter immer per Video vernommen werden, auch wenn sie in die Justizanstalt des *zuständigen* Gerichts eingeliefert wurden. § 174 Abs. 1 öStPO ist weiterhin in Kraft, gilt aber nur in Fällen einer Pandemie und ist daher seit 1.7.2023 nicht mehr anwendbar.

### *3. Haftverhandlungen (§ 176 Abs. 3 öStPO)*

Videovernehmungen des Beschuldigten waren in Pandemiezeiten nach *§ 176 Abs. 3 öStPO* auch bei *Haftverhandlungen* zulässig, wenn wegen des bevorstehenden Ab-

---

[14] ErläutRV 981 BlgNR 24. GP 93; *Kirchbacher/Keglevic*, in: Fuchs/Ratz, WK-StPO, 339. Lfg., März 2021, § 153 StPO Rn. 16; *Venier*, in: Bertel/Venier, StPO I, 2. Aufl., 2022, § 153 StPO Rn. 10.

[15] *Kirchbacher/Rami*, in: Fuchs/Ratz, WK-StPO, 319. Lfg., Mai 2020, § 172 StPO Rn. 5; *Keplinger/Prunner/Pühringer*, in: Birklbauer/Haumer/Nimmervoll/Rainer/Wess, LK-StPO, 2020, § 172 StPO Rn. 3.

[16] BGBl. I 2020/14.

[17] Aktuelle Fassung des § 174 Abs. 1 öStPO: BGBl. I 2020/16. Zur Voraussetzung „in Fällen einer Pandemie" siehe *Gölly*, Strafverfahren in Zeiten der COVID-19-Pandemie, RZ 2020, 143 (145 f.); *Stricker*, Aktuelle Änderungen durch COVID-19 im Strafrecht, ÖJZ 2020, 350 (351); *Birklbauer*, in: Resch (Hrsg.), Das Corona-Handbuch Österreichs Rechtspraxis zur aktuellen Lage, Vers. 1.06, 2020, Kap. 16 Rn. 41.

laufs der Haftfrist oder aufgrund eines Enthaftungsantrags über die Fortsetzung der Untersuchungshaft zu entscheiden war.[18] Auch diese Bestimmung ist aber nicht mehr anwendbar, weil sie auf die Fälle des § 174 Abs. 1 öStPO verweist.

*4. Kontradiktorische Vernehmungen (§ 165 Abs. 3 öStPO)*

Weitere Bestimmungen sehen den Einsatz der Videotechnologie zum *Schutz bzw. zur Schonung von Zeugen* vor:

Nach *§ 165 Abs. 3 öStPO* kann ein besonders *schutzbedürftiger Zeuge* (§ 66a öStPO) im Ermittlungsverfahren „unter Verwendung technischer Einrichtungen zur Wort- und Bildübertragung" vernommen werden.[19] Die Vernehmung wird vom sogenannten Haft- und Rechtsschutzrichter durchgeführt. Die Parteien erhalten die Gelegenheit, sich daran zu beteiligen (deshalb spricht man von einer sogenannten kontradiktorischen Vernehmung), allerdings wird die *Beteiligung der Parteien beschränkt:* Die Vernehmung wird per Video übertragen, die Parteien sind in einem anderen Zimmer als die Vernehmungsperson und die vernommene Person. Dadurch sollen dem schutzbedürftigen Opfer eine unmittelbare Konfrontation mit dem Beschuldigten und auch mehrfache Vernehmungen erspart werden, um eine „sekundäre Traumatisierung" zu vermeiden. Der Zeuge erlangt durch die kontradiktorische Vernehmung ein Aussagebefreiungsrecht (§ 156 Abs. 1 Z. 2 öStPO) und muss in der Hauptverhandlung nicht mehr aussagen. In einigen Fällen (§ 165 Abs. 4 öStPO) ist diese Art der Vernehmung sogar zwingend.[20]

Kontradiktorische Vernehmungen sind nach § 165 Abs. 1 öStPO aber nicht nur bei besonders schutzbedürftigen Zeugen, sondern immer dann vorgesehen, wenn ein Zeuge *voraussichtlich aus tatsächlichen oder rechtlichen Gründen in der Hauptverhandlung nicht zur Verfügung stehen wird.*[21] Dazu noch näher unten IV.3.a)aa).

*5. Vernehmung schutzbedürftiger Zeugen in der Hauptverhandlung (§ 250 Abs. 3 öStPO)*

Eine schonende Zeugenvernehmung per Bild- und Tonübertragung ist auch noch in der Hauptverhandlung nach § 250 Abs. 3 öStPO möglich. Wiederum geht es darum, dass ein schutzbedürftiger Zeuge nicht unmittelbar mit dem Beschuldigten im gleichen Saal konfrontiert wird, sodass der Zeuge unbefangener seine Aussage ablegen

---

[18] ErläutRV 1677 BlgNR 24. GP 12; *Pauer*, in: Birklbauer/Haumer/Nimmervoll/Rainer/Wess, LK-StPO, 2020, § 176 StPO Rn. 6; *Kirchbacher/Rami*, in: Fuchs/Ratz, WK-StPO § 176 StPO Rn. 5.

[19] *Fabrizy/Kirchbacher*, StPO, 14. Aufl., 2020, § 165 StPO Rn. 5; *Kirchbacher/Keglevic*, in: Fuchs/Ratz, WK-StPO § 165 StPO Rn. 6.

[20] *Kirchbacher/Keglevic*, in: Fuchs/Ratz, WK-StPO § 165 StPO Rn. 4; *Urbanek*, in: Birklbauer/Haumer/Nimmervoll/Rainer/Wess, LK-StPO, 2020, § 165 StPO Rn. 4, 22; *Kirchbacher/Keglevic*, in: Fuchs/Ratz, WK-StPO § 156 StPO Rn. 16.

[21] *Kirchbacher/Keglevic*, in: Fuchs/Ratz, WK-StPO § 165 StPO Rn. 8 f.; *Urbanek*, in: Birklbauer/Haumer/Nimmervoll/Rainer/Wess, LK-StPO, 2020, § 165 StPO Rn. 5 ff.

kann.[22] Derartige Vernehmungen in der Hauptverhandlung gibt es aber kaum, i. d. R. wird nur das Video der kontradiktorischen Vernehmung vorgespielt, weil der Zeuge nicht mehr zur Aussage bereit ist.

### *6. Vernehmung von Zeugen (vor allem im Ausland) in der Hauptverhandlung nach § 247a öStPO*

Eine weitere Bestimmung, die eine Zeugenvernehmung unter Verwendung technischer Einrichtungen zur Wort- und Bildübertragung *in der Hauptverhandlung* vorsieht, ist § 247a öStPO: Sie ist gedacht für Zeugen, die wegen Alter, Krankheit oder anderen erheblichen Gründen nicht vor Gericht erscheinen können oder wegen ihres Aufenthalts im Ausland und weiter Anreise nicht persönlich erscheinen wollen. Als erheblicher Grund für eine solche Art der Vernehmung gilt auch eine Gefahr für den Zeugen, die eine anonyme Vernehmung nach § 162 öStPO erlaubt. Ein solcher gefährdeter Zeuge kann also anonym bleiben, sich verkleiden und auch disloziert per Video vernommen werden.[23]

### *7. Weitere pandemiebedingte Sonderregeln*[24]

Im Zuge der Corona-Pandemie wurde zusätzlich die Möglichkeit geschaffen, in der Hauptverhandlung sowie auf Gerichtstagen in Rechtsmittelverfahren den *verhafteten Beschuldigten per Video zuzuschalten,* sofern kein ausreichend großer Verhandlungssaal verfügbar war, um die gebotenen Abstände einzuhalten (§ 239 öStPO i. d. F. BGBl. I 2020/14; § 286 Abs. 1a öStPO i. d. F. BGBl. I 2020/16).[25]

### *8. Vernehmung Jugendlicher*

Seit kurzem ist im *öJGG* die *Videoaufzeichnung der Vernehmung* vorgesehen, wenn ein Jugendlicher im Ermittlungsverfahren vernommen wird und weder ein Verteidiger noch eine Vertrauensperson anwesend ist (§ 36a Abs. 2, § 37 öJGG).

---

[22] *Kirchbacher*, in: Fuchs/Ratz, WK-StPO, 348. Lfg., Juli 2021, § 250 StPO Rn. 15 ff.; *Schmitt*, in: Birklbauer/Haumer/Nimmervoll/Rainer/Wess, LK-StPO, 2020, § 250 StPO Rn. 12 ff.

[23] *Bertel*, in: Bertel/Venier, StPO II, 2. Aufl., 2022, § 247a StPO Rn. 1; *Schmitt*, in: Birklbauer/Haumer/Nimmervoll/Rainer/Wess, LK-StPO, 2020, § 247a StPO Rn. 1, 3; *Kirchbacher*, in: Fuchs/Ratz, WK-StPO, 348. Lfg., Juli 2021, § 247a StPO Rn. 4, 6.

[24] Siehe hierzu auch *Winkelbauer-Kastner*, Vernehmung und Verhandlung via Videokonferenz: Deus ex machina im Strafprozess? JSt 2022, 326 (327 ff.).

[25] Verordnung BGBl. II 2020/113 auf Grund § 9 des 1. COVID-19-Justiz-Begleitgesetzes BGBl. I 2020/16 und 2020/24. Siehe dazu *Danek/Mann*, in: Fuchs/Ratz, WK-StPO, 346. Lfg., Juli 2021, § 239 StPO Rn. 10/1 ff. Das 1. COVID-19-Justiz-Begleitgesetz (und damit auch die auf ihrer Grundlage erlassene VO) trat mit 30.6.2023 außer Kraft (BGBl. I 2022/224). Die angeführten Sonderregeln der öStPO sind somit derzeit nicht anwendbar; im Falle des Wiederaufflammens der Pandemie könnten sie aber wieder wirksam werden, weil § 174 Abs. 1 öStPO alternativ an eine VO oder an Fälle einer Pandemie anknüpft: siehe dazu *Birklbauer*, in: Resch (Hrsg.), Corona-Handbuch, Vers. 1.06, 2020, Kap. 16 Rn. 41, 60.

*9. Zusammenfassung*

Es gibt also eine Fülle von Bestimmungen, die die Verwendung technischer Einrichtungen zur Wort- und Bildübertragung vorsehen bzw. ermöglichen. Dabei handelt es sich einerseits um audiovisuelle *Live-Vernehmungen,* andererseits um die *Aufzeichnung* von Vernehmungen per Bild und Ton, um sie in der Hauptverhandlung zu verwenden.

## III. Technische Voraussetzungen von Videovernehmungen

Zunächst zu den technischen Voraussetzungen von Videovernehmungen: Wenn eine unmittelbare Vernehmung in der Hauptverhandlung nicht möglich ist, ist eine audiovisuelle Vernehmung (Live-Vernehmung) sicher die beste Alternative oder das beste Surrogat. Sie ist jedenfalls grundsätzlich das qualitativ bessere Beweismittel als die Verlesung eines Vernehmungsprotokolls, auch wenn sie an die unmittelbare Vernehmung einer persönlich anwesenden Person nicht herankommt.[26]

Wesentliche Voraussetzung ist aber eine *qualitativ hochwertige Übertragungstechnik*. Bei schlechter Internetverbindung ruckelt das Bild, manchmal friert das Bild ganz ein, setzt die Tonverbindung vorübergehend aus oder die Verbindung reißt ganz ab, sodass Fragen und Antworten wiederholt werden müssen. Bei schlechter Tonqualität kann man Änderungen im Tonfall und in der Tonhöhe, die bei der Glaubhaftigkeitsbeurteilung u. U. eine Rolle spielen können, nicht wahrnehmen.

Ein Thema ist auch der *Bildausschnitt.* Meistens ist von der vernommenen Person nur der Kopf zu sehen. Das nonverbale Verhalten ist per Video nur eingeschränkt wahrnehmbar. Aber Details wie Körperhaltung, Mimik, Gestik, Beinbewegungen, emotionale Reaktionen usw. können für die Würdigung der Aussage bedeutungsvoll sein. § 162 öStPO, der für gefährdete Zeugen die Möglichkeit einer anonymen Vernehmung eröffnet, sieht vor, dass der Zeuge sein Gesicht nur so weit verhüllen darf, dass sein Mienenspiel noch wahrgenommen werden kann.[27] Daher sollte die Kameraeinstellung möglichst so gewählt werden, dass auch die Gestik mittels Armen und Beinen wahrnehmbar ist.[28]

Gewissen Einfluss auf die Beurteilung von Aussagen könnte auch die *Umgebung* haben, die bei der Vernehmung sichtbar ist. Ein voller Aschenbecher und Flaschen mit Alkoholika am Tisch im Hintergrund machen vermutlich einen weniger guten Eindruck als ein aufgeräumter Tisch.

---

[26] Vgl. *Deiters*, Wie viel Unmittelbarkeit braucht das Strafverfahren? Möglichkeiten und Grenzen des Beweistransfers, NJW-Beil. 2022, 43 (44); *Oberlaber/Schmollmüller*, Videoverhandlungen bzw. -vernehmungen im Spannungsverhältnis zu den Prozessgrundsätzen, JSt 2022, 340 (340 ff.).

[27] Ob und in welchem Umfang Verhaltenskriterien für die Beurteilung der Glaubhaftigkeit einer Aussage relevant sind, ist allerdings ziemlich umstritten; bedeutungsvoller sind jedenfalls inhaltliche Kriterien.

[28] Vgl. *Oberlaber/Schmollmüller*, JSt 2022, 340 (341 f.).

Die *Rahmenbedingungen* sollten jedenfalls stimmen. Wenn Zeugen bei der Vernehmung Kleinkinder am Schoß haben und durch Kinderschreie oder Läuten an der Wohnungstüre abgelenkt werden, dürfte das den Wert der Aussage beeinträchtigen. Wenn Zeugen vor Gericht erscheinen müssen, kommt das sicher nicht vor. Noch weitgehend unerforscht ist, ob es hinsichtlich des Aussageverhaltens eines Zeugen Unterschiede gibt, je nachdem, ob er unmittelbar persönlich vor Gericht seine Aussage ablegen muss oder ob er per Video vernommen wird. Es könnte sein, dass persönliche, unmittelbare Aussagen in einem Gerichtssaal auf Grund der respekteinflößenden Umgebung und der Anwesenheit von Personen im Talar einen größeren Wahrheitsgehalt haben.[29]

## IV. Videotechnologie und Prozessgrundsätze

Wie bereits zu Beginn erwähnt, wird durch die Videotechnologie vor allem der *Unmittelbarkeitsgrundsatz* tangiert, allerdings in sehr unterschiedlicher Weise.

### *1. Vernehmung von Angeklagten und Beschuldigten*

Beginnen möchte ich mit *audiovisuellen Vernehmungen des Beschuldigten oder Angeklagten* bzw. dessen *Teilnahme an Verhandlungen per Video,* was pandemiebedingt auch für Hauptverhandlungen und Verhandlungen vor dem Rechtsmittelgericht gegen *verhaftete* Angeklagte zum Schutz vor Infektionen ermöglicht wurde (§ 239 öStPO i. d. F. BGBl. I 2020/14). Der Angeklagte befindet sich dann nicht in dem Raum, in dem die vernehmende Person sitzt, bzw. ist nicht im Verhandlungssaal anwesend. Vor Corona handelte es sich in einem solchen Fall um ein Abwesenheitsverfahren, das grundsätzlich nur in den engen Grenzen des § 427 öStPO bei Vergehen zulässig ist.[30]

Eine *Hauptverhandlung,* an der der Angeklagte gerne persönlich teilnehmen würde, aber bei der er sich nur per Video einbringen kann, wirft einige rechtsstaatliche Probleme auf, auf die auch in einem Erlass[31] des Bundesministeriums vom 22.4.2020 hingewiesen wird: Demnach ist es für den bloß per Video zugeschalteten Angeklagten zweifellos *schwieriger, die Verhandlung mitzuverfolgen;* und besonders schwierig ist die *Kommunikation mit seinem Verteidiger.*

Es gibt keine Regelung, wo sich der Verteidiger aufzuhalten hat, der einen zugeschalteten Angeklagten vertritt: Bei *Hauptverhandlungen* ist für mich klar, dass der *Verteidiger im Gerichtssaal* anwesend sein muss, auch wenn sein Mandant disloziert

---

[29] Ausführlich hierzu *Schmittat*, Die Wirkung psychologischer Entscheidungsmechanismen beim Einsatz von Videotechnologie im Strafverfahren, JSt 2022, 348.

[30] RIS-Justiz RS0128200 [T1].

[31] Erlass vom 22.4.2020 über die praktische Handhabung des erweiterten Anwendungsbereichs der Durchführung von Videokonferenzen.

(in der Justizanstalt) ist. Das erforderliche Agieren des Verteidigers (z. B. ergänzendes Befragen von Zeugen, Widerspruch erheben, Anträge stellen) ist vernünftig nur bei persönlicher Anwesenheit in der Hauptverhandlung möglich.

Dadurch ist aber andererseits die *Kommunikation zwischen dem Angeklagten und seinem Verteidiger erheblich erschwert*, ganz besonders dann, wenn auch noch ein Dolmetscher nötig ist. Der Angeklagte hat ja das Recht, sich mit seinem Verteidiger zu beraten (§ 164 Abs. 2, § 245 Abs. 3 öStPO). Das ist aber sehr kompliziert, wenn der Angeklagte nicht neben seinem Verteidiger sitzt. Man muss die Hauptverhandlung immer wieder unterbrechen, damit die beiden ungestört (am ehesten per Telefon) miteinander sprechen können.[32]

Wenn der Angeklagte nur per Video an der Hauptverhandlung teilnehmen kann, ergibt sich auch ein Spannungsverhältnis zur *Waffengleichheit,* denn der Vertreter der Staatsanwaltschaft darf ja persönlich im Verhandlungssaal anwesend sein.[33] Die Präsenzverhandlung ist daher jedenfalls zu bevorzugen.

Eine ähnliche Problematik, wenn auch abgemildert, besteht bei *Vernehmungen zu den Voraussetzungen der Untersuchungshaft* und bei den parteiöffentlichen *Haftverhandlungen,* die in Pandemiezeiten fast regelmäßig per Videoschaltung von der Justizanstalt zu Gericht durchgeführt wurden (§ 174 Abs. 1, § 176 Abs. 3 öStPO). Regelungen, wo sich der Verteidiger befinden soll – ob in der Justizanstalt bei seinem Mandanten oder bei Gericht, von wo aus die Vernehmung durchgeführt wird –, gibt es auch dafür nicht. In diesen Fällen erschiene es mir naheliegend, dass der *Verteidiger beim Beschuldigten* in der Justizanstalt ist, weil die Unterstützung bei der Vernehmung im Vordergrund steht.

### *2. Audiovisuelle Vernehmung von Zeugen*

#### *a) In der Hauptverhandlung*

Die audiovisuelle Vernehmung von *Zeugen,* wie sie in *§ 247a öStPO* in der Hauptverhandlung vorgesehen ist, ist mitunter sogar die *beste Alternative* zur persönlichen, unmittelbaren Vernehmung in der Hauptverhandlung, wenn eine solche nicht möglich ist, weil dadurch das *Fragerecht* ausgeübt werden kann, mag es auch qualitativ hinter dem Fragerecht bei einer persönlichen, unmittelbaren Vernehmung zurückbleiben. Voraussetzung dafür ist natürlich eine ordentliche Übertragungsqualität. Eine Vernehmung per WhatsApp-Videoanruf mithilfe des Handys des Richters entspricht dem sicher nicht.[34]

Grundsätzlich gibt es verschiedene Möglichkeiten, eine Zeugenaussage zu erlangen, wenn ein Zeuge die Ladung zu einer Vernehmung nicht befolgt:

---

[32] *Oberlaber/Schmollmüller*, JSt 2022, 340 (345).
[33] *Oberlaber/Schmollmüller*, JSt 2022, 340 (346).
[34] *Schmittat*, JSt 2022, 348 (350 f.); *Oberlaber/Schmollmüller*, JSt 2022, 340 (346).

*Zeugen im Inland* kann man durch Beugemittel zum Kommen zwingen, man kann sie u. U. auch vorführen lassen.[35] Bei *Zeugen im Ausland* ist die Anwendung von Zwang, ja schon die bloße Androhung von Zwang unzulässig, weil dies eine Verletzung der Souveränität des ausländischen Staates wäre (siehe § 72 Abs. 1 ARHG, § 48 Abs. 1 ARHV, Art. 8 EU-RhÜbk). Wenn ein im Ausland befindlicher Zeuge der Ladung (die nach Art. 5 Abs. 1 EU-RhÜbk mit internationalem Rückschein zugestellt werden kann) nicht befolgt, besteht die Möglichkeit, die Beweisperson im *Rechtshilfeweg* durch eine ausländische Strafverfolgungsbehörde vernehmen zu lassen, allenfalls mithilfe einer Europäischen Ermittlungsanordnung (EEA: §§ 55 ff. EU-JZG; § 55h), und das *Protokoll* über diese Vernehmung in der Hauptverhandlung zu verlesen.

Eine der materiellen Unmittelbarkeit aber zweifellos besser entsprechende Möglichkeit ist eine *Videokonferenz nach § 247a Abs. 2 öStPO,* also eine Vernehmung per Videoschaltung, die allerdings – abgesehen von der Zustimmung der Parteien[36] – eine entsprechende Kooperation der Behörden des anderen Staates und technische Voraussetzungen erfordert.[37]

Eine derartige Vernehmung *sollte* – zumindest bei wichtigen Zeugen – *immer versucht* werden, und sie sollte – anders als derzeit – auch zulässig sein, wenn die ausländischen Behörden keine Rechtshilfe leisten. Nur subsidiär sollte, wenn eine Videovernehmung trotz Bemühungen nicht zustande kommt, auf ein Protokoll zurückgegriffen werden.[38]

Die öStPO spricht allerdings nur davon, dass die Vernehmung eines Zeugen auf diese Weise erfolgen kann. Es ist nach herrschender Ansicht also grundsätzlich zulässig und kein Verfahrensfehler, wenn gleich ein vorhandenes Vernehmungsprotokoll aus dem Ermittlungsverfahren in der Hauptverhandlung verlesen wird. Denn § 252 Abs. 1 Z. 1 öStPO erklärt die Verlesung eines Protokolls für zulässig, wenn das persönliche Erscheinen des Zeugen aus erheblichen Gründen nicht bewerkstelligt werden konnte, und das trifft auf Zeugen im Ausland zu, wenn eine Ladung versucht, ihr aber nicht Folge geleistet wurde.[39]

Das Gericht ist nach herrschender Ansicht in Rechtsprechung und Lehre *nicht verpflichtet, von Amts wegen eine Videovernehmung zu organisieren.* Allerdings kann der Angeklagte bzw. sein Verteidiger bei einer bloßen Verlesung des Protokolls das *Fragerecht* nicht ausüben. Das kann nach der Rechtsprechung des EGMR eine Verletzung des *fair trial*-Gebotes (Art. 6 EMRK) darstellen, wenn es sich um einen

---

[35] *Danek/Mann*, in: Fuchs/Ratz, WK-StPO § 242 StPO Rn. 2 ff.

[36] Das Fernbleiben des Angeklagten bedeutet keine (konkludente) Zustimmung: OGH 13.6.2023, 11 Os 54/23k; 11 Os 55/23g; 11 Os 56/23d; 11 Os 57/23a.

[37] *Hinterhofer*, Videovernehmungen und deren Verwertbarkeit im österreichischen Strafprozess, RZ 2000, 234 (238); *Sautner*, Videotechnologie im Strafverfahren: Kommunikation, Dokumentation und Reproduktion, JBl 2019, 210 (214 ff.); *Divjak*, JSt 2024, 319 (329).

[38] Siehe auch *Schmoller*, in: Fuchs/Ratz, WK-StPO § 13 StPO Rn. 28; *Bertel*, in: Bertel/Venier, StPO II, 2. Aufl., 2022, § 247a StPO Rn. 1; *Deiters*, NJW-Beil. 2022, 43 (44).

[39] *Kirchbacher*, in: Fuchs/Ratz, WK-StPO § 252 StPO Rn. 64.

wichtigen Belastungszeugen handelt und keine ausreichenden Kontrollbeweise (flankierende Beweise) vorhanden sind.[40]

Nach der *Judikatur des OGH* steht es den Parteien frei, eine audiovisuelle Vernehmung in der Hauptverhandlung zu *beantragen*. Die Ablehnung eines diesbezüglichen Antrags kann zur Urteilsnichtigkeit führen, wenn dadurch Verteidigungsrechte des Beschuldigten gemäß Art. 6 EMRK verletzt wurden.[41] Das ist wiederum dann der Fall, wenn keine ausreichenden Kontrollbeweise vorhanden sind. Diesfalls muss also dem Antrag entsprochen und eine Videovernehmung zumindest versucht werden. Wünschenswert wäre aber eine Verpflichtung des Gerichts, eine Videovernehmung zu versuchen.

Diese Verlagerung der bestmöglichen Sachverhaltsaufklärung auf die Parteien ist ständige Judikatur des OGH. Nach Ansicht des OGH ist die sogenannte Aufklärungsrüge nach § 281 Abs. 1 Z. 5a öStPO ein subsidiäres Rechtsmittel. Sie kann nur dann mit Aussicht auf Erfolg erhoben werden, wenn der Verteidiger oder die Staatsanwaltschaft an der Stellung eines Antrags gehindert war.[42] Diese Rechtsprechung erachte ich als problematisch und wird auch immer wieder kritisiert: Wenn man die Pflicht des Gerichts zur amtswegigen Wahrheitserforschung ernst nimmt, sollte die Videovernehmung eines ausländischen Zeugen nicht von einem Antrag abhängig gemacht werden.

### *b) Im Ermittlungsverfahren*

Eine audiovisuelle Vernehmung von Zeugen, die in einem anderen Sprengel wohnen, kann nach *§ 153 Abs. 4 öStPO auch im Ermittlungsverfahren* erfolgen. Das ist eher unproblematisch, weil es sich dabei um keine parteiöffentliche Vernehmung handelt und die Person außerdem i. d. R. persönlich in der Hauptverhandlung erscheinen muss, um ihre Aussage abzulegen.[43]

---

[40] EGMR, Urt. v. 28.8.1992 – Rs. 39/1991/291/362 (Artner/Österreich) ÖJZ-MRK 1992/41, 846; EGMR, Urt. v. 15.12.2015 – Rs. 9154/10 (Schatschaschwili/Deutschland); siehe auch RIS-Justiz RS0074930; *Fuchs*, Zur Verwertung polizeilicher Ermittlungen im Strafprozeß, in: FS für Franz Pallin, 1989, 81 (88); *Kirchbacher*, in: Fuchs/Ratz, WK-StPO § 252 StPO Rn. 25 f. Anders ist die Situation, wenn der ausländische Zeuge im Ermittlungsverfahren kontradiktorisch unter Beteiligung der Parteien vernommen wurde, weil schon absehbar war, dass er nicht zur Hauptverhandlung persönlich erscheinen würde, sodass das Fragerecht zumindest in einem früheren Verfahrensstadium eingeräumt wurde.

[41] OGH 10.3.2015, 11 Os 154/14b (Ablehnung eines Antrags der StA auf Durchführung einer Videovernehmung nach § 247a Abs. 2 öStPO); *Bertel*, in: Bertel/Venier, StPO II, 2. Aufl., 2022, § 247a StPO Rn. 1; *Kirchbache*r, in: Fuchs/Ratz, WK-StPO § 247a StPO Rn. 11; *Ratz*, in: Fuchs/Ratz, WK-StPO, 379. Lfg., Februar 2024, § 281 StPO Rn. 336 f.

[42] OGH 13.9.2000, 13 Os 99/00; 18.5.2022, 13 Os 35/22d; 9.12.2020, 13 Os 35/20a = RIS-Justiz RS0115823; *Ratz*, in: Fuchs/Ratz, WK-StPO § 281 StPO Rn. 480.

[43] *Kirchbacher/Keglevic*, in: Fuchs/Ratz, WK-StPO § 153 StPO Rn. 16; *Venier*, in: Bertel/Venier, StPO I, 2. Aufl., 2022, § 153 StPO Rn. 10.

Wenn sich ein Zeuge im Ausland befindet, ist § 153 Abs. 4 öStPO nicht anwendbar. Es besteht jedoch zwischen Mitgliedstaaten der EU die Möglichkeit einer Vernehmung per Videokonferenz im Rechtshilfeweg gemäß § 55h EU-JZG.[44]

### *3. Bild-Ton-Aufzeichnungen von Vernehmungen zur späteren Vorführung in der Hauptverhandlung*

#### *a) Kontradiktorische Vernehmung von Zeugen im Ermittlungsverfahren (§ 165 Abs. 3 öStPO)*

##### *aa) Schutzbedürftige Zeugen*

*Schutzbedürftige Zeugen* werden regelmäßig im Ermittlungsverfahren kontradiktorisch unter Verwendung technischer Einrichtungen zur Wort- und Bildübertragung vernommen, wobei die *Beteiligung der Parteien beschränkt wird* (§ 165 Abs. 3 öStPO). Die Parteien können ihr Fragerecht nicht direkt ausüben, sondern die Fragen werden der Vernehmungsperson übermittelt, die die Fragen sozusagen für die Parteien stellt. Minderjährige Opfer von Sexualdelikten sind sogar zwingend auf diese Weise zu vernehmen (§ 165 Abs. 4 öStPO). Wenn sich besonders schutzbedürftige Opfer einer solchen Vernehmung einmal gestellt haben, erlangen sie nach der österreichischen Rechtslage ein *Aussagebefreiungsrecht* (§ 156 Abs. 1 Z. 2 öStPO). Machen sie von diesem Recht Gebrauch, werden sie zur Hauptverhandlung gar nicht mehr geladen, die Videoaufzeichnung dieser kontradiktorischen Vernehmung wird in der Hauptverhandlung vorgeführt (§ 252 Abs. 1 Z. 2a öStPO).

Ein *Antrag auf ergänzende Vernehmung* eines kontradiktorisch vernommenen Opfers ist aussichtslos, auch wenn sich *neue, erheblich geänderte Verhältnisse,* z. B. wesentliche neue Beweise *nach* der kontradiktorischen Vernehmung, ergeben haben. Der Zeuge ist nach der Rechtsprechung des OGH[45] *absolut und dauerhaft von der Aussagepflicht befreit* (§ 156 Abs. 1 Z. 2 öStPO), sodass ihm die neuen Beweisergebnisse zwecks näherer Aufklärung nicht vorgehalten werden können. Nur hinsichtlich neuer, später hinzugekommener Taten, auf die sich die kontradiktorische Vernehmung nicht bezogen hat, steht dem Zeugen kein Aussagebefreiungsrecht zu.

In einer Entscheidung aus dem Jahr 2014[46] hatte der OGH noch eine andere Auffassung vertreten: Eine ergänzende Vernehmung eines bereits kontradiktorisch vernommenen Zeugen sei auch dann geboten, wenn nach einer solchen Vernehmung ein neues Beweissubstrat (zum selben Faktum) hinzukommt, das außerhalb des bisherigen Aussageinhalts steht (Aussagepflicht in diesem Umfang). Im Jahr 2017[47] ist der OGH davon aber wieder abgegangen. Nach neuerer Rechtsprechung „können neue

---

[44] *Kirchbacher/Keglevic*, in: Fuchs/Ratz, WK-StPO § 153 StPO Rn. 17. Kritisch dazu *Divjak*, JSt 2024, 319 (327 f.), der *de lege ferenda* eine Ausweitung des § 154 Abs. 4 öStPO auf Zeugen und Beschuldigte im Ausland vorschlägt.

[45] OGH 6.12.2017, 13 Os 120/17x.

[46] OGH 15.1.2015, 12 Os 152/14s JBl 2015, 608 (zust. *Schwaighofer*).

[47] OGH 6.12.2017, 13 Os 120/17x.

Beweisergebnisse (nur) Kontrollbeweise als zulässig erscheinen lassen". Was das heißen soll, bleibt im Dunkeln. Eine Pflicht des Zeugen, sich einer ergänzenden Vernehmung zu unterziehen, wird jedenfalls abgelehnt mit der dürftigen Begründung, dass das Zeugnisverweigerungsrecht dem Opferschutz diene (was niemand in Zweifel zieht).

Diese Judikatur erscheint rechtsstaatlich nicht vertretbar: Es geht um eine vernünftige *Ausbalancierung der Bedürfnisse des Opferschutzes einerseits und der Verteidigungsrechte* des Beschuldigten (*fair trial*) und des Gebots der Ermittlung der materiellen Wahrheit andererseits. Wenn sich nach einer kontradiktorischen Vernehmung neue Umstände ergeben, die bei der früheren Vernehmung nicht berücksichtigt werden konnten und nach Aufklärung durch Konfrontation des Zeugen mit diesen Beweisergebnissen verlangen, dann ist es nicht vertretbar, eine ergänzende Befragung in der Hauptverhandlung, die vielleicht Monate nach der Vernehmung stattfindet, kategorisch für unzulässig zu erklären (es sei denn das Opfer würde sich dazu bereit erklären).[48]

Richtigerweise müsste im Fall neuer Beweisergebnisse *im Einzelfall entschieden* werden, ob das Interesse der materiellen Wahrheitserforschung durch ergänzende Vernehmung gegenüber dem Interesse des Opfers, keine neuerliche belastende Vernehmung über sich ergehen lassen zu müssen, überwiegt. Wenn die Interessen der Wahrheitserforschung überwiegen und keine Gefahr eines schwerwiegenden Nachteils für das Opfer besteht, muss das Aussagebefreiungsrecht des Opfers zurücktreten (wie das auch in Deutschland der Fall ist).[49] Das Gesetz lässt es ohne weiteres zu, das Aussagebefreiungsrecht gemäß § 156 Abs. 1 Z. 2 öStPO in diesem Sinn auszulegen, wie das auch der OGH in der Entscheidung 12 Os 152/14s getan hat. Den Interessen der Wahrheitserforschung und dem Fragerecht des Beschuldigten wird allein durch die Beteiligungsgelegenheit mit Fragerecht bei einer (frühen) kontradiktorischen Vernehmung oft nicht ausreichend entsprochen.[50] Und noch einmal ist darauf hinzuweisen, dass es ja auch die Möglichkeit der schonenden Vernehmung in der Hauptverhandlung nach § 250 Abs. 3 öStPO gibt.

Hinzu kommt, dass das *Fragerecht* bei derartigen kontradiktorischen Vernehmungen wegen der beschränkten Beteiligung auch nicht im üblichen Umfang ausgeübt werden kann.

Während sich bei einer *unmittelbaren Befragung* von Zeugen eine *Gesprächsdynamik* entwickeln kann, wird diese Dynamik bei einer *abgesonderten Vernehmung* verhindert: Durch die mittelbare Befragung über den Richter (bzw. Sachverständigen) kann kein Gesprächsfluss („*Ductus*") zustande kommen. Zurechtgelegte Befragungskonzepte sind unrealisierbar, das Stellen naheliegender, an eine Antwort anknüpfender Ergänzungsfragen, das sofortige Hinweisen auf Widersprüche und

[48] *Ignor*, in: Thesen, 22 (25).

[49] *Ignor*, in: Thesen, 22 ff.; *Deiters*, NJW-Beil. 2022, 43 (46).

[50] Siehe hierzu auch *Schwaighofer*, Zur ergänzenden Vernehmung von nach § 156 Abs. 1 Z. 2 StPO aussagebefreiten Zeugen, JSt 2022, 238.

Vorhalte, um die Glaubhaftigkeit der Aussage des Opfers zu erschüttern, sind nicht möglich.[51] Besonders stark beeinträchtigt ist die Ausübung des Fragerechts, wenn die Fragen nicht direkt (über eine Kabelverbindung) der Vernehmungsperson übermittelt werden können, sondern *schriftlich* formuliert werden müssen und von der Vernehmungsperson abgeholt werden.

Weiters besteht bei einer abgesonderten Vernehmung die Gefahr, dass *Fragen* des Beschuldigten oder Verteidigers an den Zeugen von der Vernehmungsperson derart *umformuliert* werden, dass sie nicht mehr den intendierten Inhalt haben und an Wert verlieren. Das gilt besonders bei der Vernehmung kindlicher Opfer: In diesen Fällen sind die Vernehmungspersonen naturgemäß bestrebt, besonders schonungsvoll vorzugehen („kindgerechte Übersetzung") und eine lockere Gesprächsatmosphäre zu schaffen. Wie dem Zeugen die Frage von der Vernehmungsperson genau gestellt wird, darauf hat der „Auftraggeber" praktisch keinen Einfluss.[52]

Ein weiteres Problem – die *Verteidigung* bei kontradiktorischen Vernehmungen – wurde vor einigen Jahren immerhin entschärft. Der Beschuldigte ist selbst ja nicht vernünftig in der Lage, sein Fragerecht auszuüben. Seit 2016 besteht für kontradiktorische Vernehmungen in Verfahren mit Verteidigerzwang in der Hauptverhandlung notwendige Verteidigung (§ 61 Abs. 1 Z. 5a öStPO i. d. F. StPRÄG I 2016). Damit hat der Beschuldigte nun auch Anspruch auf Beigebung eines Verfahrenshelfers, wenn er sich keinen Verteidiger leisten kann (§ 61 Abs. 2 Z. 1 in Verbindung mit § 61 Abs. 1 Z. 5a öStPO).

*bb) Kontradiktorische Vernehmungen*

Kontradiktorische Vernehmungen mit Videoaufzeichnung sind nach § 165 Abs. 1 öStPO generell vorgesehen, wenn ein Zeuge *voraussichtlich aus tatsächlichen oder rechtlichen Gründen in der Hauptverhandlung nicht zur Verfügung stehen wird.*

Das betrifft z. B. Zeugen, die im Ausland wohnhaft sind und voraussichtlich nicht zur Hauptverhandlung anreisen werden. Und das trifft auch auf *angehörige Zeugen* zu, bei denen es immer wieder vorkommt, dass sie zwar zunächst, gleich im Anschluss an eine Anzeige, aussagebereit sind und einen Angehörigen belasten, einige Zeit später jedoch, wenn es zur Hauptverhandlung kommt, aus welchen Gründen auch immer (z. B. zur Wahrung des Familienfriedens) von ihrem Aussagebefreiungsrecht Gebrauch machen. Dies führt nach österreichischer Rechtslage dazu, dass *Protokolle* über frühere Aussagen, mögen sie auch völlig korrekt zustande gekommen

---

[51] *Schwaighofer/Giacomuzzi*, Die kontradiktorische Vernehmung, 2019, Teil 1 Rn. 119 ff.; *Machan*, in: Kier/Wess (Hrsg.), Handbuch Strafverteidigung, 2. Aufl., 2022, Rn. 4.38.

[52] Unter Umständen werden bestimmte Fragen, die als „zu hart" angesehen werden, gar nicht gestellt oder es werden Fragen leicht suggestiv gestellt, ohne dass der Verteidiger dagegen sofort protestieren kann: *Oberschlick*, Thesen aus dem Panel: Das Problem der mittelbaren Befragung im Rahmen der kontradiktorischen Vernehmung, JSt 2013, 15 (Bericht über die Thesen des 11. Österreichischen StrafverteidigerInnentags 2013 in Graz).

sein, in der Hauptverhandlung *nicht verlesen werden dürfen*.[53] Der angehörige Zeuge kann also gewissermaßen über seine frühere Aussage disponieren und dadurch mittelbar den Beschuldigten vor Strafverfolgung schützen. Es dürfen bei sonstiger Nichtigkeit auch keine anderen Beweissurrogate herangezogen werden: Es ist in Österreich – anders als in Deutschland – also auch unzulässig, eine Vernehmungsperson über den Inhalt der Aussage zu befragen, weil dies eine Umgehung des Zeugnisverweigerungsrechts darstellt.[54]

Das Verbot der Verwendung eines Surrogats gilt jedoch dann *nicht,* wenn das Opfer bei einer kontradiktorischen Vernehmung im Ermittlungsverfahren ausgesagt hat, bei der die Parteien Gelegenheit zur Beteiligung hatten. Die Aufzeichnung dieser Vernehmung darf nach § 252 Abs. 1 Z. 2a öStPO in der Hauptverhandlung vorgeführt und verwendet werden.

Hier stellt sich für mich die grundsätzliche rechtspolitische Frage, ob angehörigen Zeugen die Möglichkeit eingeräumt werden soll, frühere Aussagen von der Verwendung auszuschließen: Soll man den Interessen des angehörigen Zeugen an der *Wahrung des Familienfriedens* den *Vorrang* vor dem Interesse an der Wahrheitsermittlung einräumen und ihm dieses Dispositionsrecht (zumindest bei erwachsenen Personen) zugestehen?[55] Wenn man diese Frage bejaht, dann müsste das aber immer gelten, auch wenn die Parteien bei einer kontradiktorischen Vernehmung im Ermittlungsverfahren Gelegenheit zur Ausübung des Fragerechts hatten.[56] Das Zeugeninteresse ist nämlich das Gleiche.

Will man umgekehrt der *Wahrheitserforschung den Vorrang* einräumen, dann müsste man die Verlesung früherer Aussagen, die nach korrekter Belehrung über das Aussagebefreiungsrecht zustande gekommen sind, wohl grundsätzlich zulassen. Dass der Beschuldigte das Fragerecht nicht ausüben konnte, wäre dann bei der Beweiswürdigung zu berücksichtigen, so wie das auch bei Zeugen der Fall ist, die inzwischen verstorben sind oder deren Anwesenheit in der Hauptverhandlung nicht bewerkstelligt werden kann: Es müssen also, um dem *fair trial* zu entsprechen, ausreichend Kontrollbeweise vorhanden sein.

### *b) Bild-Ton-Aufzeichnung von Beschuldigtenvernehmungen*

Immer wenn eine Videoaufzeichnung einer früheren Vernehmung die *unmittelbare Vernehmung ersetzen* soll, dann steht das in einem deutlichen Spannungsverhältnis zu Prozessgrundsätzen und sollte deshalb nur sehr zurückhaltend zugelassen werden.

*Anders* ist das freilich, wenn Bild-Ton-Aufzeichnungen die *unmittelbare Vernehmung ergänzen* sollen. Die ergänzende Vorführung solcher Aufzeichnungen dient

---

[53] *Venier*, in: Bertel/Venier, StPO I, 2. Aufl., 2022, § 165 StPO Rn. 2.

[54] *Kirchbacher*, in: Fuchs/Ratz, WK-StPO § 252 StPO Rn. 109; *Fabrizy/Kirchbacher*, StPO, 14. Aufl., 2020, § 252 StPO Rn. 26 f.

[55] Bei Unmündigen wird man das anders handhaben müssen.

[56] *Cirener*, in: Thesen, 20.

jedenfalls der Wahrheitserforschung und beeinträchtigt keine Verteidigungsrechte. Insofern erschiene es sinnvoll, Vernehmungen aufzuzeichnen, um die Aufzeichnung im Fall des Falles ergänzend heranziehen zu können.

Die *Aufzeichnung von Beschuldigtenvernehmungen* im Ermittlungsverfahren, die regelmäßig von der Polizei durchgeführt werden, ist zwar nach § 97 öStPO zulässig, aber bei erwachsenen Beschuldigten grundsätzlich nicht geboten. Nur wenn dem Beschuldigten für seine Vernehmung die Beiziehung eines Verteidigers verwehrt wird, um eine erhebliche Gefahr für die Ermittlungen abzuwenden, ist „nach Möglichkeit" eine Ton- oder Bildaufnahme gemäß § 97 öStPO anzufertigen (§ 164 Abs. 2 letzter Satz öStPO).

Eine obligatorische Aufzeichnung einer Beschuldigtenvernehmung ist nur bei *Jugendlichen* in bestimmten Fällen vorgesehen: § 37 öJGG sieht seit 2020 vor, dass ein festgenommener Jugendlicher bei seiner Vernehmung immer durch einen Verteidiger vertreten sein muss. Bei sonstigen Vernehmungen von jugendlichen Verdächtigen muss eine Vertrauensperson anwesend sein, und wenn eine solche nicht verfügbar ist, ist die Vernehmung zwingend in Bild und Ton aufzuzeichnen (§ 36a Abs. 2 öJGG).

Meines Erachtens wäre eine Bild-Ton-Aufzeichnung von Beschuldigtenvernehmungen *generell sinnvoll,* damit *ergänzend* zur unmittelbaren Vernehmung in der Hauptverhandlung diese Tonaufzeichnung im Bedarfsfall verfügbar ist, die präzise und authentisch wiedergibt, was die vernommene Person wie gesagt hat und auch wie die Befragung erfolgt ist.

Wenn der Beschuldigte in der Hauptverhandlung eine Aussage ablegt, die von seiner früheren Aussage im Ermittlungsverfahren laut Vernehmungsprotokoll abweicht, dann wird regelmäßig das Protokoll nach § 245 öStPO verlesen und ihm vorgehalten. Aber jedes Protokoll ist subjektiv gefärbt: Die Vernehmungsperson protokolliert, wie sie die Angaben wahrgenommen hat. Es ist auch notwendig lückenhaft und verkürzt. Manche Vernehmungsprotokolle sind geradezu haarsträubend. Kollege *Scheil* hat mir vor ein paar Jahren ein Protokoll gezeigt, in dem ein Beschuldigter gesagt haben soll: „Ich habe es […] ernstlich für möglich gehalten und mich damit abgefunden, den XY schwer zu verletzen." Es ist geradezu auszuschließen, dass der Beschuldigte das selbst so gesagt hat. Die Protokolle der ersten Vernehmung vor der Polizei, bei denen im Übrigen nur selten ein Verteidiger anwesend ist, haben für die Beweiswürdigung aber große Bedeutung. Und wehe, der Angeklagte erklärt die Abweichung damit, dass seine Aussage von der Polizei falsch protokolliert worden sein muss. Das führt nicht selten zu einem zusätzlichen Strafverfahren wegen Verleumdung (Vorwurf des Amtsmissbrauchs oder der unrichtigen Protokollierung im Amt). Eine Aufzeichnung kann die Polizisten übrigens auch vor falschen Anschuldigungen schützen; man kann einen Vorwurf rasch klären, ohne die vernehmenden Polizisten vorladen zu müssen.[57]

---

[57] Siehe hierzu auch *Untch/Wrobel*, Chancen und Risiken der virtuellen Vernehmungssituation, JSt 2022, 319 (319 f.).

Wichtig ist natürlich, dass wirklich die gesamte Vernehmung aufgezeichnet wird (§ 97 Abs. 1 öStPO) und *keine Vorgespräche* vor dem Einschalten des Aufnahmegeräts stattgefunden haben. Diese Gefahr könnte man dadurch minimieren, dass der Beschuldigte zu Beginn der Aufzeichnung immer zu fragen ist, ob irgendwelche Vorgespräche mit dem Vernehmungsbeamten stattgefunden haben. Und die Aufzeichnung müsste natürlich auch vor späterer Manipulation geschützt werden, etwa durch gemeinsame Versiegelung gleich nach Beendigung der Vernehmung.[58]

## V. Zusammenfassung

Der Unmittelbarkeitsgrundsatz hat einen hohen Wert und sollte daher unangetastet bleiben. Die persönliche, unmittelbare Vernehmung ist jedem Surrogat, auch der Videovernehmung, vorzuziehen. Wenn man die Verwendung von Surrogaten erleichtert, dann wird – psychologisch verständlich – davon auch Gebrauch gemacht, weil die Verhandlungen schneller zu einem Ende kommen. Auch von der für Pandemiezeiten geschaffenen Möglichkeit, den Angeklagten bloß per Video zur Hauptverhandlung zuzuschalten, sollte möglichst sparsam Gebrauch gemacht werden. Videovernehmungen sind allerdings eine wertvolle Alternative, wo sich die formelle Unmittelbarkeit nicht realisieren lässt, und sollten vorrangig angestrebt werden, bevor bloß ein Aussageprotokoll verlesen wird.

Das Vorführen von Videoaufzeichnungen *anstelle* einer an sich möglichen unmittelbaren Vernehmung sollte nur in absoluten Ausnahmefällen zugelassen werden, weil Verteidigungsrechte dadurch stark beschränkt werden. Opferschutz kann eine solche Ausnahme darstellen, er darf aber nicht so weit gehen, wie dies die Rechtsprechung des OGH ermöglicht. Als *ergänzendes* Beweismittel – zusätzlich zur unmittelbaren Vernehmung – wäre die Aufzeichnung von Vernehmungen aus meiner Sicht sogar wünschenswert.

[58] *Untch/Wrobel*, JSt 2022, 319 (321 ff.).

# Die „Sicherstellung“ von Daten

## Insbesondere durch elektronischen Zugriff auf externe Datenspeicher

*Andreas Venier*



## I. Das Gesetz, die Materialien, die Problematik

Die öStPO kennt verschiedene Möglichkeiten, um an verfahrensrelevante Informationen zu gelangen. Eine aus forensischer Sicht besonders ergiebige Methode besteht in der Sicherstellung von Datenträgern (z. B. PC, Festplatte, Laptop, Mobiltelefon) mit dem Ziel, mutmaßlich beweiserhebliches Datenmaterial zu sichern und auszuwerten. Unter einer Sicherstellung versteht die öStPO (§ 109 Z. 1 lit. a) „die vorläufige Begründung der Verfügungsmacht über Gegenstände“. § 111 Abs. 2 öStPO nimmt Bezug auf elektronische Daten, die auf Datenträgern „sichergestellt“ werden sollen. In diesem Fall muss „jedermann Zugang zu diesen Informationen gewähren“ und „auf Verlangen einen elektronischen Datenträger in einem allgemein gebräuchlichen Dateiformat ausfolgen oder herstellen lassen“. Außerdem muss er/sie es dulden, dass Kriminalpolizei und Staatsanwaltschaft Sicherungskopien von den auf dem Datenträger gespeicherten Informationen herstellen.

Zu § 111 Abs. 2 öStPO findet sich in den Gesetzesmaterialien[1] folgende Erläuterung:

„Elektronische Daten sind immaterielle Objekte und bedürfen für ihre Existenz materieller Verkörperung. Eine Suche nach Daten ist daher untrennbar an die vorhergehende Suche nach entsprechenden Datenträgern verknüpft."

Das bedeutet, wenig überraschend, dass Daten als Gegenstand der Sicherstellung nur in Verbindung mit einem Datenträger existieren. Daten sind eben keine „Gegenstände", die man in seine „Verfügungsmacht" bringen kann. So werden in Wahrheit – anders als § 111 Abs. 2 öStPO suggeriert – nicht die Daten, sondern die Datenträger, auf denen sie gespeichert sind, „sichergestellt".[2] Die Materialien geben ferner zu bedenken, dass es „insbesondere im Bereich vernetzter Rechnersysteme" zu Schwierigkeiten bei der Auffindung von Daten kommen könne, nämlich dann, wenn man „auf dem eigentlich durchsuchten Rechner" keine relevanten Datenbestände vorfinde, weil diese auf einem „im Netzverbund befindlichen Datenserver" gespeichert sind. Dann, so die Materialien, komme es auf die Kenntnis der „Netzwerkarchitektur" an, und dann sei die von der Maßnahme betroffene Person verpflichtet, jene Handlungen vorzunehmen, die „den Zugang zu auf Datenträgern gespeicherten Informationen" gewährleisten. Die entscheidende Frage aber, durch welche „Handlungen" der Betroffene den Zugang zu welchen Speichermedien eröffnen muss, lassen die Materialien unbeantwortet.

Nach h. M. verschafft man den Strafverfolgungsorganen den Zugang zu Daten, indem man ihnen vorzugsweise sein Wissen über Passwörter und sonstige Zugangsschlüssel preisgibt.[3] Eine darüber hinausgehende Beratertätigkeit muss man nicht entfalten, insbesondere den Ermittlern nicht die Funktionsweise eines Programms erklären.[4] Wer tatverdächtig ist, den treffen jedoch weder Informations- noch Herausgabepflichten. Der Beschuldigte ist nicht verpflichtet, mit den Strafverfolgungsbehörden zusammenzuarbeiten oder sie sogar mit selbstbelastenden Informationen oder Beweismitteln zu versorgen (§ 7 Abs. 2 öStPO).[5]

---

[1] ErläutRV 25 BlgNR 22. GP 156.

[2] Vgl. *Keplinger/Prunner/Pühringer*, in: Birklbauer/Haumer/Nimmervoll/Wess (Hrsg.), StPO. Linzer Kommentar zur Strafprozessordnung, 2020, § 111 StPO Rn. 6.

[3] *Tipold/Zerbes*, in: Fuchs/Ratz (Hrsg.), Wiener Kommentar zur Strafprozessordnung, 345. Lfg., März 2021, § 111 StPO Rn. 13/1; *Keplinger/Prunner/Pühringer*, in: Birklbauer/Haumer/Nimmervoll/Wess, LK-StPO, 2020, § 111 StPO Rn. 8; *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht Cyberdelikte und Ermittlungsbefugnisse, 2018, Rn. 5.9.

[4] I.d.S. *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht, 2018, Rn. 5.9; *Tipold/Zerbes*, in: Fuchs/Ratz, WK-StPO § 111 StPO Rn. 13/1; *Kroschl*, in: Schmölzer/Mühlbacher (Hrsg.), StPO Strafprozessordnung I, 2. Aufl., 2021, § 111 StPO Rn. 11.

[5] *Venier*, in: Bertel/Venier (Hrsg.), StPO-Kommentar I, 2. Aufl., 2022, § 111 StPO Rn. 2; *Tipold/Zerbes*, in: Fuchs/Ratz, WK-StPO § 111 StPO Rn. 13/1; *Keplinger/Prunner/Pühringer*, in: Birklbauer/Haumer/Nimmervoll/Wess, LK-StPO, 2020, § 111 StPO Rn. 8; *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht, 2018, Rn. 5.9; *Fabrizy/Kirchbacher*, StPO und wichtige Nebengesetze, 14. Aufl., 2020, § 111 StPO Rn. 7. Auch Zeugnisverweigerungsberechtigte oder von der Aussage befreite Personen sind dazu nicht verpflichtet, siehe *Kroschl*, in: Schmölzer/Mühlbacher, StPO I, 2. Aufl., 2021,

Deutlich schwieriger zu beantworten ist die Frage nach den Speicherplätzen, deren Daten zugänglich gemacht werden sollen. In der Entscheidung des OGH 14 Os 51/18h geht es um Fotos aus einer Überwachungskamera, die auf der Festplatte eines Geldausgabeautomaten abgespeichert sind und mutmaßlich den Täter beim unberechtigten Abheben von Bargeld zeigen. Die Verfügungsmacht über den Automaten samt der darin installierten Festplatte liegt gewöhnlich beim Automatenaufsteller, also i. d. R. bei Payment Services Austria (PSA). Dieser Aufsteller kann z. B. eine Kopie der Fotos auf einem USB-Stick herausgeben, um eine Sicherstellung der Festplatte des Bankomaten abzuwenden (§ 111 Abs. 2 öStPO). Die Bank, die dem Aufsteller den Platz zum Aufstellen des Automaten zur Verfügung stellt, hat normalerweise keinen Zugriff auf die Festplatte im Automateninneren, falls aber doch, muss sie den Strafverfolgungsbehörden den Zugang zu diesen Fotos ermöglichen oder, was den Interessen der Bank mehr entgegenkommt,[6] die relevanten Fotos auf einen Datenträger kopieren und diesen der ermittelnden Behörde aushändigen. In diesem Sinn betont der OGH in der besagten Entscheidung, dass auch derjenige den Strafverfolgungsbehörden den Zugriff auf elektronisch gespeicherte Daten verschaffen muss, der über den Datenträger selbst nicht verfügt, aber in der Lage ist, den Zugang zu den Daten zu eröffnen.

Der OGH geht insoweit über den Anlassfall hinaus, als er seine Aussage ganz allgemein auf externe Speicherplätze erweitert. Danach soll der Betroffene den Zugang auch zu Daten ermöglichen, die mit Hilfe von Cloud-Computing- oder Cloud-Storage-Diensten auf entfernte Datenserver ausgelagert wurden. Das hat weitreichende Folgen: Cloud-Computing ist mittlerweile eine gängige Methode, um große Datenmengen außerhalb des eigenen, begrenzten Speichermediums zu konservieren. Bei handelsüblichen Mobiltelefonen – heute ganz überwiegend Smartphones – geschieht diese Form der Datenspeicherung zumeist automatisch, also ohne Tätigwerden des Gerätenutzers, ja vielfach ohne dass es diesem bewusst ist. Um zu verhindern, dass das Mobiltelefon von sich aus von allen möglichen Datenverarbeitungsvorgängen eine Cloud-Speicherung (Cloud-Backup) anfertigt, muss der Nutzer diese Funktion deaktivieren. Tut er dies nicht, sind grundsätzlich alle in der Cloud oder Rechnerwolke gespeicherten Daten, z. B. Nachrichten, Fotos, Videos und Chats, dem Berechtigten und jedem, der das Mobiltelefon mittels PIN aktivieren kann, zugänglich. Das bedeutet, dass der Berechtigte – wenn er nicht gleichzeitig der Verdächtige ist – diesen Zugang nach Ansicht des OGH auch den Strafverfolgungsbehörden verschaffen muss, indem er für sie einen Datenträger mit diesen Daten herstellt, der dann als „materielle Verkörperung" der Daten sichergestellt werden kann. Doch was geschieht, wenn sich der Berechtigte – zulässig oder unzulässig – weigert, den Strafverfolgungsbehörden den Zugang zu diesen Daten auf diese Weise zu eröff-

---

§ 111 StPO Rn. 4 f.; *Tipold/Zerbes*, in: Fuchs/Ratz, WK-StPO § 111 StPO Rn. 9; *Kirchbacher*, StPO und wichtige Nebengesetze, 15. Aufl., 2024, § 111 StPO Rn. 3.

[6] So auch der OGH in der genannten Entscheidung.

nen? Darf sich dann die Kriminalpolizei, allenfalls auf Anordnung des Staatsanwalts, diesen Zugang selber verschaffen, z. B. indem sie mit Hilfe eines Entschlüsselungsprogramms den PIN des zuvor sichergestellten Mobiltelefons knackt,[7] die über das Internet zugänglichen Daten mittels Fernzugriff aus der Cloud absaugt und für die Strafverfolgung sichert? Der OGH jedenfalls scheint eher der Ansicht zu sein, dass Daten „der materiellen Verkörperung" bedürfen, damit sie als Objekte einer Sicherstellung in Frage kommen. Das würde auch auf den vorliegenden Fall passen, weil die Bank der Staatsanwaltschaft einen USB-Stick mit Kopien der Überwachungsbilder aushändigte. Dieser USB-Stick konnte als Beweisgegenstand problemlos sichergestellt werden.

## II. „Sicherstellung" durch virtuellen Zugriff auf externe Datenspeicher?

Nach dem Gesetzmäßigkeitsgrundsatz (§ 5 Abs. 1 öStPO) muss jede behördliche oder richterliche Befugnis zu Eingriffen in Rechte von Personen „gesetzlich ausdrücklich" vorgesehen sein. Ausdrücklich vorgesehen ist die Befugnis zur Begründung der Verfügungsmacht über den Datenträger, in dem sich die Daten, wie es die Materialien formulieren, „materiell" verkörpern. § 111 Abs. 2 öStPO erweitert die Sicherstellung von Datenträgern um die Befugnis, von „jedermann" zu verlangen, Zugang zu „auf Datenträgern gespeicherten Daten" zu gewähren und „einen elektronischen Datenträger in einem allgemein gebräuchlichen Datenformat" auszuhändigen oder herstellen zu lassen, gemeint ist: einen Datenträger mit einer „materiellen Verkörperung" der Daten, deren Zugang gewährt werden muss, damit er anstelle des Originaldatenträgers sichergestellt werden kann. Eine Befugnis der Strafverfolgungsorgane, selber auf externe Datenspeicher, die nicht in ihrer Verfügungsmacht stehen, über ein sichergestelltes Mobiltelefon zuzugreifen, gibt der Gesetzestext jedoch nicht her. Diese Form des Datenzugriffs wird, wie in der Literatur mit Recht betont, der „gegenstandsbezogenen Bindung der Sicherstellung" nicht gerecht.[8] Denn damit werden in die Sicherstellung dieses einen Datenträgers – hier des Mobiltelefons – nachträglich Speicherplätze einbezogen, auf die sich die gegenstandsbezogene Verfügungsmacht nicht erstreckt. Die Begründung einer lediglich virtuellen „Verfügungsmacht", z. B. über das Internet, ist definitionsgemäß gerade keine Sicherstellung.

Anders liegt der Fall, wenn es sich um Daten handelt, die auf dem Handy selbst gespeichert sind. Diese Daten sind ein mit dem Gerät verbundener Inhalt und gehen

---

[7] Zur Frage des erzwungenen Zugriffs auf biometrisch verschlüsselte Endgeräte *Flörl*, Erzwungener Zugriff auf Daten auf biometrisch verschlüsselten Endgeräten? ZWF 2021, 12 (insb. 15); mit beachtlichen Argumenten gegen die Zulässigkeit einer derartigen Zwangsmaßnahme *Seidl/Schönborn*, Dürfen Strafverfolgungsbehörden Beschuldigte zur (biometrischen) Entschlüsselung von Endgeräten zwingen? JBl 2022, 361 (366 f.).

[8] *Zerbes*, Beweisquelle Handy, ÖJZ 2021, 176 (178).

mit der Sicherstellung des Geräts in die Verfügungsmacht der Behörde über, so wie der Inhalt eines sichergestellten Schriftstücks, Tagebuchs oder Fotoalbums.[9]

Aus den gesetzlichen Regeln über die Sicherstellung lässt sich demnach kein Recht der Behörde ableiten, selbst virtuell auf externe Datenspeicher zuzugreifen. Daran ändert auch die Aussage der Materialien[10] nichts, dass der Betroffene der Behörde den Zugang zu Daten auch dann verschaffen müsse, wenn die relevanten Datenbestände nicht „auf dem eigentlich durchsuchten Rechner", sondern auf einem „im Netzverbund befindlichen Datenserver" gespeichert sind. Zwar haben die Strafverfolgungsbehörden das Recht, die Hilfe des Betroffenen in Anspruch zu nehmen, wenn sie auf einen Rechner „im Netzverbund" zugreifen wollen. Die Informationen des Betroffenen können der Behörde helfen, den Rechner sicherzustellen, seine Daten auszulesen, Datenkopien anzufertigen oder die Ausfolgung eines Datenträgers, z. B. eines USB-Sticks, mit den Kopien der Daten zu verlangen und dann diesen Datenträger sicherzustellen. Doch ein von der Praxis derzeit praktiziertes „weites Verständnis des § 111 Abs. 2" wonach man diese Bestimmung als „Ergänzung der auf körperliche Verfügungsmacht beschränkten Sicherstellung" verstehen müsse, die es der Behörde ermögliche, die Untersuchung des sichergestellten Computers auf Daten auszuweiten, die nur online erreicht werden können, findet auch unter Einbeziehung der Materialien keine Deckung im Gesetz.[11]

## III. Die Ähnlichkeit des virtuellen Fernzugriffs mit Datenauskunft und Nachrichtenüberwachung

Es bleibt dabei: Die Regeln über die Sicherstellung geben Behörden und Gerichten keine Befugnis, die Datenbestände eines nicht sichergestellten Rechners ohne die Einwilligung der Berechtigten abzusaugen. Diese Art des virtuellen Fernzugriffs auf Daten hat vielmehr Ähnlichkeit mit anderen Formen des Datenzugriffs und der Datenauswertung.

Zu denken ist an die „Auskunft über Daten einer Nachrichtenübermittlung" (§ 134 Z. 2 öStPO) und die „Überwachung von Nachrichten" (§ 134 Z. 3 öStPO): Mit der Datenauskunft verbindet man üblicherweise die Rufdatenerfassung, z. B. um einen Drohanruf nachverfolgen zu können; mit der Nachrichtenüberwachung das Abhören von Telefongesprächen, z. B. um einen mutmaßlichen Drogenhändler überführen zu können. Aber beide Maßnahmen sind umfassender als es diese Beispiele vermuten

---

[9] *Zerbes/Ghazanfari*, Stellungnahme im Auftrag des Instituts für Anwaltsrecht der Universität Wien zur Sicherstellung und Auswertung von Daten und Datenträgern, AnwBl 2022, 640 (641); ebenso *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht, 2018, Rn. 5.11.

[10] ErläutRV 25 BlgNR 22. GP 156.

[11] Diesem Problem wird auch durch das Abstellen auf eine „auf diesen externen Datenbestand bezogene Sicherstellungsanordnung" nicht abgeholfen; vgl. aber *Tipold/Zerbes*, in: Fuchs/Ratz, WK-StPO § 111 StPO Rn. 14/2.

lassen. So geht es im Fall der „Auskunft über Daten einer Nachrichtenübermittlung" um Daten, die während einer Kommunikation beim Telekommunikations- oder Internetanbieter anfallen, z. B. die aktive und passive Teilnehmernummer, der Zeitpunkt und die Dauer der Verbindung, der Standort des Nutzers.[12] Diese Verkehrs-, Zugangs- und Standortdaten erlangt die Behörde durch ein Auskunftsverlangen beim Telekommunikations- oder Internetanbieter.

Eingriffsintensiver ist die „Überwachung von Nachrichten". Auch daran hat der Telekommunikations- oder Internetanbieter mitzuwirken. Es handelt sich dabei um die Überwachung von Kommunikationsinhalten, die über ein öffentliches Telekommunikationsnetz oder das Internet transportiert werden. Die Kommunikation kann in einer Nachricht (z. B. Telefongespräch, SMS, E-Mail) oder in einer Information (§ 134 Z. 3 öStPO) bestehen, z. B. im Aufruf einer Webseite oder in der Übertragung von Daten in eine Cloud. In der Literatur wird diese Form der Kommunikation als „Kommunikation im technischen Sinn" bezeichnet, weil sie im Unterschied zur „Kommunikation im sozialen Sinn" nicht im Austausch von Gedanken zwischen Personen besteht.[13] Allerdings ähnelt die Preisgabe dieser Kommunikation mitunter eher der Auskunft über Daten einer Nachrichtenübermittlung als einer echten Überwachung von Nachrichten, etwa wenn nur erhoben werden soll, welche Internetseiten aufgerufen oder ob und wann Daten in eine Cloud verschoben wurden. Um ein aktuelles Beispiel zu nennen: Es macht einen Unterschied, ob die Auskunft nur darin bestehen soll, ob Thomas Schmid und Sebastian Kurz zu einer gewissen Zeit miteinander gechattet haben, oder ob auch die Inhalte dieser Chats mitgeliefert werden sollen. In dem einen Fall bezieht sich die Auskunft lediglich auf die Tatsache der Kommunikation zwischen Schmid und Kurz, in dem anderen auch auf den Kommunikationsinhalt. Ein von den Strafverfolgungsbehörden begehrter Zugriff auf Chatprotokolle in einer Cloud im Sinn einer nachträglichen Auskunft über den Kommunikationsinhalt kommt der Überwachung von Nachrichten gleich. Auch wenn man beim Wort „überwachen" in erster Linie an das Abhören, Aufzeichnen oder Abfangen von aktuell gesendeten, übermittelten oder empfangenen Kommunikationsinhalten denkt, lässt es sich auch als Abfrage, Durchsicht oder Speicherung längst gesendeter oder empfangener Nachrichten verstehen.

Kommunikationsdaten, die auf dem Gerät selbst, z. B. dem Smartphone oder Laptop, gespeichert sind, gelten zwar auch als Daten einer Nachrichtenübermittlung, werden aber nach herrschender Ansicht der „Sphäre" des betroffenen Geräteinhabers zugerechnet und unterliegen wie andere Informationen, die auf einem Datenträger oder den Unterlagen des Betroffenen gespeichert bzw. verschriftlicht sind, den Regeln der Sicherstellung von körperlichen Sachen.[14] Das gilt auch für die auf diesen

[12] *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht, 2018, Rn. 5.71 ff.

[13] *Zerbes/Ghazanfari*, AnwBl 2022, 640 (642) im Anschluss an *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht, 2018, Rn. 5.102.

[14] *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht, 2018, Rn. 5.6; *Zerbes/Ghazanfari*, AnwBl 2022, 640 (641).

Geräten gespeicherten Nachrichteninhalte, z. B. Chats, SMS, E-Mails.[15] Die Unterscheidung ist deshalb von Bedeutung, weil die Auskunft über Daten einer Nachrichtenübermittlung und die Überwachung der Kommunikation deutlich strengeren formellen und materiellen Regeln unterliegen als die bloße Sicherstellung des Geräts beim Geräteinhaber.

Für die Sicherstellung des Datenträgers braucht die Polizei, wenn es sich nicht gerade um eine geringwertige (Wert nicht über 100 €) oder um eine „vorübergehend leicht ersetzbare" Sache handelt (§ 110 Abs. 3 Z. 1 lit. d öStPO), eine Anordnung des Staatsanwalts. „Leicht ersetzbar" und/oder geringwertig kann z. B. ein USB-Stick mit Datenkopien sein.[16] Auf ein Mobiltelefon oder einen Laptop wird das eher nicht zutreffen. So benötigt die Polizei in diesem Fall eine Anordnung des Staatsanwalts (§ 110 Abs. 2 öStPO), dieser jedoch benötigt für seine Sicherstellungsanordnung keine Bewilligung des Richters, auch wenn er oder die Polizei alle Daten auf dem sichergestellten Datenträger, z. B. dem Handy oder Laptop, auslesen, kopieren und für Zwecke der Strafverfolgung verwenden. Eine richterliche Bewilligung würde es nur brauchen, wenn der Datenträger im Wege einer Hausdurchsuchung[17] sichergestellt werden sollte.[18] Für die Sicherstellung selbst genügt jedoch auch im Fall einer Hausdurchsuchung eine schlichte Anordnung des Staatsanwalts. Eine gewisse Schwere der aufzuklärenden Tat oder einen qualifizierten Verdacht schreibt das Gesetz weder für Hausdurchsuchungen noch für Sicherstellungen vor. Grundsätzlich kommt jedes Delikt für eine Hausdurchsuchung oder Sicherstellung in Frage, theoretisch auch der Anfangsverdacht eines Ladendiebstahls.

Demgegenüber erfordern die Auskunft über Daten einer Nachrichtenübermittlung und die Überwachung der Kommunikation in formeller Hinsicht eine richterliche Bewilligung und in materieller Hinsicht eine gewisse Tatschwere: Die Auskunft über Daten einer Nachrichtenübermittlung muss für die Aufklärung einer Vorsatztat erforderlich sein, die mit mehr als einem Jahr oder, falls der Geräteinhaber der Auskunft durch den Diensteanbieter zustimmt, mit mehr als sechs Monaten Freiheitsstrafe bedroht ist (§ 135 Abs. 1 Z. 1, § 137 Abs. 1 öStPO). Für die Überwachung von Kommunikationsinhalten (z. B. das Abhören von Telefonaten, der Abruf von Nachrichten auf der Mobilbox und das Mitlesen des E-Mailverkehrs)[19] sind noch weitere Einschränkungen zu beachten. So muss etwa der Inhaber des überwachten Geräts der mit mehr als einem Jahr Freiheitsstrafe bedrohten Vorsatztat dringend verdächtig sein (§ 135 Abs. 3 Z. 3 lit. a öStPO). Überdies droht für den Fall, dass eine der beiden

---

[15] § 111 Abs. 2 öStPO spricht hier von der Sicherstellung der „auf Datenträgern gespeicherten Informationen".

[16] OGH 11.9.2018, 14 Os 51/18h.

[17] Durchsuchung von Wohnungen und anderen vom Hausrecht geschützten Räumlichkeiten, z. B. Arztpraxen und Betriebsräume von Unternehmen (§ 117 Z. 2 lit. b öStPO).

[18] § 119 Abs. 1, § 120 Abs. 1 öStPO.

[19] *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht, 2018, Rn. 5.6.

Maßnahmen nicht „rechtmäßig" bewilligt oder angeordnet wurde, ein Verwendungsverbot (§ 140 Abs. 1 Z. 2 öStPO).

## IV. Ist das unterschiedliche Schutzniveau bei der Sicherstellung von Datenträgern einerseits und bei der Datenauskunft und Nachrichtenüberwachung andererseits berechtigt?

Die im Vergleich zur Sicherstellung erheblich strengeren Voraussetzungen für die „Auskunft über Daten einer Nachrichtenübermittlung" und die „Überwachung von Nachrichten" erklären sich zum Teil dadurch, dass diese Maßnahmen geheim und ohne Kenntnis des Betroffenen stattfinden. Dieser erfährt erst im Nachhinein, dass seine Kommunikation überwacht bzw. seine Kommunikationsdaten den Strafverfolgungsbehörden bekanntgegeben wurden. Die Sicherstellung dagegen geschieht gleichsam unter den Augen des Betroffenen, ihm gegenüber ist keine Geheimhaltung zulässig, im Gegenteil, er muss sofort oder binnen 24 Stunden eine Bestätigung über die Sicherstellung erhalten, damit er sie ehestmöglich beeinspruchen oder bei Gericht deren Aufhebung begehren kann (§ 111 Abs. 4 öStPO). Für den wirksamen Gebrauch dieser Rechtsschutzinstrumentarien ist es allerdings von entscheidender Bedeutung, dass der Betroffene nicht nur erfährt, welche Datenträger sichergestellt wurden, sondern auch welche Dateien mit welchen Inhalten davon betroffen sind. Eine solche Detailinformation stößt auf praktische Schwierigkeiten, wenn auf dem Datenträger viele Dateien und große Datenmengen gespeichert sind. Denkbar wäre immerhin die Übergabe einer Kopie des gesamten auf dem Datenträger gespeicherten Datenbestands. Dem Vernehmen nach soll dies jedoch bei Smartphones in vertretbarer Zeit nur möglich sein, wenn der PIN zum Entsperren des Geräts schon bekannt ist.[20] In der Regel könne sich der Betroffene einen Überblick über seine Daten erst verschaffen, wenn sie von der Behörde ausgewertet worden sind und der verfahrensrelevante Inhalt verschriftlicht und zum Akt genommen worden ist.[21] Das kann je nach Datenumfang und Art der Datenverschlüsselung Monate dauern. Bis dahin sind die Dateninhalte auch für den Betroffenen nicht einsehbar und daher mehr oder weniger – ähnlich den Überwachungsergebnissen einer Telefonüberwachung – unbekannt.

Das offene Vorgehen der Strafverfolgungsbehörden bei der Sicherstellung sollte daher nicht überbewertet werden und vor allem nicht darüber hinwegtäuschen, dass die Sicherstellung von Datenträgern ähnlich schwer in Grundrechte der Betroffenen eingreift wie Datenauskunft und Nachrichtenüberwachung. Der mit der Sicherstellung des Datenträgers verbundene Eingriff in das Eigentum ist vielleicht noch das

[20] Näher *Zerbes/Ghazanfari*, Sicherstellung und Verwertung von Handy-Daten. Reformperspektiven, AnwBl 2023, 549 (561).

[21] *Zerbes/Ghazanfari*, AnwBl 2023, 549 (560 f.).

geringste Übel. Viel gravierender wiegen zumeist die Eingriffe in das Recht auf Privat- und Familienleben (Art. 8 EMRK) und das Grundrecht auf Datenschutz (§ 1 DSG), wenn z. B. vertrauliche Chats oder Fotos an Dritte, hier Staatsanwalt und Kriminalpolizei, gelangen und der Betroffene vorläufig keinen Zugriff mehr auf diese Daten hat. Zu bedenken ist auch die große Streuwirkung solcher Eingriffe in dem Sinn, dass viele der ausgelesenen Daten mit dem aufzuklärenden Tatverdacht wenig bis gar nichts zu tun haben[22] und viele Kommunikationspartner grundlos in den Sog der Ermittlungen geraten, es aber doch hinnehmen müssen, dass den Ermittlern – und über Umwege oft auch den Medien – sehr private und intime Umstände bekannt werden.

Schwer wiegt auch der Eingriff in Geschäfts- und Berufsgeheimnisse, zu deren Geheimhaltung der Betroffene im Interesse von Kunden, Patienten oder Klienten berechtigt, ja verpflichtet ist. Zum Schutz der Verschwiegenheitsrechte von Psychologen, Psychiatern, Rechtsanwälten, Journalisten und anderen Berufsgeheimnisträgern, deren gesetzlich anerkanntes Verschwiegenheitsrecht bei sonstiger Nichtigkeit nicht umgangen werden darf, hat der Gesetzgeber in § 112 öStPO Vorkehrungen getroffen. Die schriftlichen Aufzeichnungen und Datenträger dieser Berufsgeheimnisträger dürfen nämlich nur soweit eingesehen, ausgelesen und kopiert werden, als die Inhalte nicht vom Verschwiegenheitsrecht umfasst sind. Dies zu prüfen und zu beurteilen, obliegt dem Gericht, nicht der Polizei und nicht der Staatsanwaltschaft. Für andere Verschwiegenheitsberechtigte, z. B. praktische Ärzte, oder für Personen, die an der Geheimhaltung ihrer Daten und Dateien „nur" ein berechtigtes privates oder berufliches Interesse geltend machen können, bestehen keine vergleichbaren Schutzvorschriften.

Ein gutes Beispiel, um die Problematik zu verdeutlichen, ist wieder das Smartphone. Es ist Kommunikations-, Datenverarbeitungs- und Speichermedium in einem und gibt unvergleichlich tiefe Einblicke in das Leben einer Person. Die auf dem Gerät selbst und in der Cloud als Backup im Laufe der Zeit gespeicherten Fotos, Videos, Nachrichten, Chats, Internetaufrufe usw. ergeben ein Bild der beruflichen und privaten Aktivitäten, der persönlichen, auch sexuellen Vorlieben, der religiösen und weltanschaulichen Präferenzen einer Person, wie es kaum ein anderes Medium schaffen könnte. Ein Tagebuch beispielsweise kann sich vielleicht literarisch, aber nicht in der Dichte der Informationen mit dem elektronischen Datensammler „Smartphone" messen. Außerdem: Wer vertraut heute noch seine Erlebnisse, Meinungen und Gefühle dem altmodischen Tagebuch an? Im Vergleich zu den unzähligen Usern von Smartphones kann es sich nur um eine verschwindende Minderheit handeln.

Es zeigt sich also, dass die mit der Sicherstellung von Datenträgern verbundenen Grundrechtseingriffe häufig eine Intensität erreichen, die jener einer „Überwachung von Nachrichten" (§ 134 Z. 3 öStPO) oder einer „Auskunft über Daten einer Nach-

[22] Die Chatnachrichten im Fall Schmid gingen in die Hunderttausende und enthielten dem Vernehmen nach auch viele intime Mitteilungen und Fotos.

richtenübermittlung“ (§ 134 Z. 2 öStPO) gleichkommt. So mutet es zunehmend anachronistisch an, wenn die Sicherstellung von Datenträgern so gesehen wird, als handle es sich bei Smartphones und anderen Endgeräten lediglich um die digitale Ausgabe von Papieren, Tagebüchern oder anderen schriftlichen Unterlagen. Dies gilt besonders, wenn die Sicherstellung im Widerspruch zur gesetzlichen Definition dafür eingesetzt wird, sich über den sichergestellten Datenträger einen virtuellen Zugang zu externen Datenspeichern (Stichwort Cloud) zu verschaffen.

## V. Zwischenbilanz

Die geltenden Vorschriften über die Sicherstellung wurden 2004 beschlossen[23] und traten im Jänner 2008 mit der Reform des Ermittlungsverfahrens in Kraft. Damals waren der Versand und das Abspeichern großer Datenmengen über Mobiltelefone technisch noch nicht ausgereift und nach heutigen Maßstäben auch nicht üblich. Die Gesetzverfasser dachten zwar an „vernetzte Computer“,[24] aber nicht an die massenhafte, alltägliche Anwendung von Smartphones, Laptops und ähnlichen Geräten, die viele der damaligen Computersysteme gemessen an ihrer Speicherkapazität, Verarbeitungsgeschwindigkeit und Netzanbindung in den Schatten stellen. Auch massentaugliche Cloudspeichersysteme kamen erst später auf. Der Gesetzgeber konnte die rasante Entwicklung auf diesen Gebieten schwerlich vorhersehen und demgemäß auch nicht ermessen, welche Bedeutung sie einmal für die Gesellschaft und den Einzelnen haben werden. Dass sich die Gesetzesverfasser vorsichtshalber „technologieneutraler“ Formulierungen bedienten und sich auch später davor scheuten, nötige Anpassungen vorzunehmen, weil man angeblich nicht ständig hinter den technischen Neuerungen „hinterherhinken“ wolle,[25] ändert nichts an diesem Befund.

Die Sicherstellung von Endgeräten, mit denen elektronische Kommunikation gesendet und empfangen werden kann (z. B. Smartphone, Smartwatch, PC, Laptop), sollte zumindest ähnlichen Beschränkungen unterworfen sein wie die Überwachung von Nachrichten oder die Auskunft über Daten einer Nachrichtenübermittlung, je nachdem ob Kommunikationsinhalte oder nur äußere Kommunikationsdaten abgefragt werden. Grundsätzlich sollte die Maßnahme nur nach richterlicher Bewilligung und nur bei gewisser Tatschwere durchgeführt werden dürfen[26] und ihre Ergebnisse

---

[23] Strafprozessreformgesetz BGBl. I 2004/19.

[24] ErläutRV 25 BlgNR 22. GP 156.

[25] So der Leiter der Legistik im BMJ *Christian Manquet* am 22.6.2023 in der mündlichen Verhandlung vor dem VfGH; zitiert aus https://www.puls24.at/news/politik/vfgh-verhandlung-zu-sichergestellten-smartphones/300636 (Abrufdatum: 9.7.2024).

[26] Für das Erfordernis einer noch näher zu definierenden „schwerwiegenden Tat“ *Pilnacek*, Wieviel Rechtsstaatlichkeit verträgt die Strafrechtspflege? ZWF 2023, 50 (57); weniger streng mittlerweile *Zerbes/Ghazanfari*, AnwBl 2023, 549 (560), die eine „Anlasstat-Schwelle“ nicht mehr für „sachgerecht“ halten und den Richtervorbehalt um eine „Gefahr im Verzug“-Regelung ergänzen wollen.

sollten nur verwertbar sein, wenn sie rechtmäßig angeordnet und bewilligt wurde. Nicht vertretbar ist jedenfalls eine Fortführung der derzeit praktizierten Umdeutung der geltenden gegenstandsbezogenen Form der Sicherstellung in ein virtuelles Fernzugriffsrecht auf externe Datenspeicher. Hier wird eindeutig eine Grenze überschritten, die mit der Definition der Sicherstellung als „vorläufige Begründung der Verfügungsmacht über Gegenstände" nicht mehr vereinbar ist. Dass die Strafverfolgungsbehörde über die Sicherstellung eines Handys ohne weiteres auf die Cloud-Backups der vergangenen Jahre zugreifen kann,[27] ist indiskutabel. Wenigstens für diese Form des Datenzugriffs braucht es eine ausdrückliche gesetzliche Ermächtigung und erheblich strengere materielle und formelle Zulässigkeitsvoraussetzungen als für eine gewöhnliche Sicherstellung.

## VI. Die neusten Entwicklungen

### *1. Das Erkenntnis des VfGH vom 14.12.2023*[28]

Die vorhin angestellten Überlegungen entsprechen der Rechtslage im Zeitpunkt des Vortrags, den der Verfasser am 20.11.2023 im Rahmen der Ringvorlesung „Internationalisierung und Digitalisierung – Herausforderungen für das Recht" an der Universität Innsbruck gehalten hat. Nunmehr zwingt ein Erkenntnis des VfGH den Gesetzgeber zu einer grundlegenden Überarbeitung der Sicherstellungsbestimmungen bis zum 31.12.2024. Der VfGH erklärt nämlich wesentliche, die Sicherstellung betreffende Bestimmungen für verfassungswidrig und verfügt ihr Außerkrafttreten mit Ende 2024.[29]

Die grundrechtliche Problematik der derzeitigen Sicherstellungsregeln zeigt sich nach Ansicht des VfGH vor allem darin, dass sie eine nahezu schrankenlose Auswertung aller auf einem Datenträger „intern oder extern" gespeicherten Inhalte erlauben, das heißt aller Daten, die am Datenträger gespeichert sind oder über ihn von einem externen Speicherplatz (Netzwerksystem, Cloud) abgerufen werden können.[30] Der VfGH erwähnt ausdrücklich Smartphone, Laptop, Notebook, PC und andere IT-Endgeräte, deren Sicherstellung „einen umfassenden Einblick in wesentliche Teile des bisherigen und aktuellen Lebens" der Betroffenen ermöglicht.[31] Auf diese Weise können „umfassende Persönlichkeits- und Bewegungsprofile" von verdächti-

---

[27] In der Praxis wird das Smartphone im Zeitpunkt der Sicherstellung auf „Flugmodus" geschaltet, damit „nur" auf die bereits gespeicherten Daten zugegriffen werden kann; näher *Prior*, Sicherstellung und Auswertung elektronischer Daten, AnwBl 2023, 554 (555).

[28] VfGH 14.12.2023, G 352/2021.

[29] Davon betroffen sind § 110 Abs. 1 Z. 1, Abs. 4 und § 111 Abs. 2 öStPO.

[30] Eingehend VfGH 14.12.2023, G 352/2021, Rn. 37 ff., 95 ff.; zu den Entscheidungsgründen auch *Soyer/Marsch*, VfGH zur Handysicherstellung, JSt 2024, 118 (120 f.).

[31] VfGH 14.12.2023, G 352/2021, Rn. 35, 70, 66.

gen und unverdächtigen Kommunikationsteilnehmern erstellt werden.[32] Die in der öStPO für die Sicherstellung von Datenträgern vorgesehenen Anforderungen und Schutzmechanismen reichen nach Überzeugung des VfGH nicht aus, um die Betroffenen wirksam vor überschießenden oder unangemessenen Eingriffen in die Grundrechte auf Datenschutz (§ 1 Abs. 1 DSG) und Achtung des Privat- und Familienlebens (Art. 8 EMRK) zu schützen.[33] Für eine verfassungskonforme Novellierung wird der Gesetzgeber auf die im Erkenntnis formulierten Leitlinien verwiesen.

Grundbedingung für die Sicherstellung und anschließende Auswertung eines Datenträgers ist nach Ansicht des VfGH eine richterliche Bewilligung, die festlegt, welche Datenkategorien mit welchen Inhalten aus welchen Zeiträumen für welche Zwecke ausgewertet werden dürfen.[34] Ein Richtervorbehalt „bloß zu Beginn" biete aber noch keinen ausreichenden Rechtsschutz.[35] Abhängig von der Intensität des Eingriffs müssen weitere Anforderungen an die Sicherstellung und Auswertung von Datenträgern hinzutreten. So verlangt der VfGH die Berücksichtigung „insbesondere" folgender „Gesichtspunkte":[36] Es mache einen Unterschied, ob der Gesetzgeber die Sicherstellung von Datenträgern und die Auswertung der darauf (lokal oder extern) gespeicherten Daten bei einem Anfangsverdacht einer Straftat „unabhängig von ihrer Schwere, von dem mit dem Straftatbestand geschützten Rechtsgut oder von dem bei der Begehung einer Straftat typischerweise eingesetzten Datenträger (‚Cyberkriminalität')" oder aber „nur bei bestimmten Straftaten" ermögliche.[37] Wesentlich seien außerdem Vorkehrungen zum Schutz vor unnötiger und unverhältnismäßiger Auswertung von Datenbeständen, und die Betroffenen müssten „in geeigneter Weise" jene Informationen erhalten, die sie zur Wahrung ihrer Rechte in einem laufenden Ermittlungs- oder Hauptverfahren befähigen.[38] Für „bedeutsam" hält der VfGH auch „effektive Maßnahmen einer unabhängigen Aufsicht", vor allem darüber, ob bei der Auswertung der Daten die gesetzlichen Vorschriften eingehalten und die Rechte der Betroffenen gewahrt werden.[39]

### *2. Der Entwurf eines Strafprozessrechtsänderungsgesetzes 2024*[40]

Der Entwurf[41] bezweckt (u. a.) die Umsetzung der vom VfGH geforderten verfassungskonformen Neuregelung der Sicherstellung von Datenträgern und der Auswertung der darauf (lokal oder extern) gespeicherten Daten. Er spricht von „Beschlagnahme von Datenträgern und Daten" und definiert sie als „eine gerichtliche Entschei-

[32] VfGH 14.12.2023, G 352/2021, Rn. 66 f.
[33] VfGH 14.12.2023, G 352/2021, Rn. 86 ff.
[34] VfGH 14.12.2023, G 352/2021, Rn. 78 f.
[35] VfGH 14.12.2023, G 352/2021, Rn. 96.
[36] VfGH 14.12.2023, G 352/2021, Rn. 98.
[37] VfGH 14.12.2023, G 352/2021, Rn. 99.
[38] VfGH 14.12.2023, G 352/2021, Rn. 100 f.
[39] VfGH 14.12.2023, G 352/2021, Rn. 102.
[40] ME Strafprozessrechtsänderungsgesetz 2024, 349/ME 27. GP.
[41] Deckungsgleich mit dem Initiativantrag 4125/A.

dung auf Begründung einer Sicherstellung" zum „Zweck der Auswertung" von: a) Datenträgern und darauf gespeicherten Daten, b) Daten, die an anderen Speicherorten als einem Datenträger gespeichert sind, soweit auf sie von diesem aus zugegriffen werden kann, oder c) Daten, die auf Datenträgern gespeichert sind, die zuvor für andere Zwecke sichergestellt wurden (§ 109 Z. 2a öStPO-Entw.). Eine Sicherstellung von Datenträgern zu anderen Zwecken, z. B. zur Beweissicherung darauf befindlicher physischer Spuren, zur Sicherung des Verfalls oder von Opferansprüchen, fällt hingegen unter die allgemeine Sicherstellungsregel nach § 109 Z. 1 lit. a öStPO-Entw. Die Erläuterungen[42] erwähnen als Beispiel die Sicherstellung von Fahrzeugen mit integrierten Datenträgern zur Sicherung privatrechtlicher Ansprüche. Dies leuchtet ein, weil die Bedenken des VfGH ja der Sicherstellung von Datenträgern wie Laptop, Notebook, PC, Smartphone und „sonstigen IT-Endgeräten" gelten (VfGH G 352/2021, Rn. 35, 41, 66, 70). Dabei handelt es sich typischerweise um Geräte zur Übermittlung und Speicherung digitaler Kommunikation[43] (siehe auch III.). Die Bedenken des VfGH beziehen sich offensichtlich nicht auf die Sicherstellung von Fahrzeugen, Maschinen und Haushaltsgeräten, in denen Prozessoren und Datenspeicher integriert sind, die lediglich technische Vorgänge steuern, gewisse Werte messen und speichern, z. B. Verbrauch, Temperatur, Zeit und Dauer der Nutzung. Obwohl man auch diese Geräte für „digitale Endgeräte" halten könnte,[44] werden auf ihnen üblicherweise keine Kommunikationsvorgänge oder personenbezogenen Daten gespeichert. Der Gesetzesvorschlag differenziert allerdings nicht nach der (potentiellen) Eignung von Daten, ernstzunehmende Rückschlüsse auf die Gewohnheiten und die Persönlichkeit der Nutzer zuzulassen:[45] Sobald Daten ausgewertet werden sollen, handelt es sich nach dem Entwurf stets um eine Beschlagnahme von Datenträgern und Daten, für die künftig ausschließlich die Regeln der neu geschaffenen §§ 115f–115l und nicht die allgemeinen Sicherstellungsregeln für Gegenstände und Vermögenswerte gelten sollen. Eine „vorsorgliche" Sicherstellung von Datenträgern nach den Regeln der Sicherstellung, um die gespeicherten Daten bei Bedarf auslesen zu können, ist nach den Erläuterungen unzulässig.[46]

Der Entwurf wendet die neuen Beschlagnahmeregeln auch auf Daten an, die an einem anderen Speicherort als dem beschlagnahmten Datenträger gespeichert sind, soweit von diesem Datenträger aus auf sie zugegriffen werden kann (§ 109 Z. 2a lit. b öStPO-Entw.). Damit will der Gesetzesvorschlag eine ausdrückliche gesetzliche Rechtsgrundlage für den Fernzugriff auf externe Speichermedien (z. B. Cloud-Diens-

---

[42] 349/ME 27. GP Erläut. 11.

[43] Das gilt im Übrigen auch für die zunehmend beliebten Smartwatches.

[44] Vgl. etwa § 4 Z. 10 IKT-Schulverordnung (BGBl. II 2021/382): Danach sind „digitale Endgeräte" Einrichtungen zur elektronischen oder nachrichtentechnischen Übermittlung, Speicherung und Verarbeitung von Sprache, Text, Stand- und Bewegtbildern sowie Daten, die zur Datenverarbeitung und -kommunikation eingesetzt werden können, insbesondere Notebooks oder Tablets.

[45] Vgl. VfGH 14.12.2023, G 352/2021, Rn. 67 f.

[46] 349/ME 27. GP Erläut. 10 ff.

te) schaffen;[47] er kommt damit der unter V. erhobenen Forderung nach Verrechtlichung nach.

Der Entwurf bezieht grundsätzlich alle Datenträger in die neuen Beschlagnahmevorschriften ein, sofern sie „zum Zweck der Auswertung von Daten" sichergestellt werden, mit einer Ausnahme: Daten, die „mittels Bild- und Tonaufzeichnungsgeräten an öffentlichen oder öffentlich zugänglichen Orten" aufgenommen wurden, sollen weiterhin nach allgemeinen Regeln sichergestellt werden können (§ 111 Abs. 2 öStPO-Entw.). Danach ist „jede Person" verpflichtet, Zugang zu diesen Daten zu gewähren. Die Erläuterungen[48] begründen dies damit, dass hier keine Auswertung der Daten stattfinde, weil nur Videomaterial sichergestellt werden soll, das ein „bestimmtes Geschehen festhält". Es sollen „somit" nicht der „gesamte Datenträger und sämtliche Daten" sichergestellt werden, sondern der Eingriff in das Grundrecht auf Datenschutz (§ 1 DSG) und das Recht auf Achtung des Privat- und Familienlebens (Art. 8 EMRK) solle nur „punktuell" erfolgen. Da durch solche Aufnahmen nicht die Gefahr drohe, dass mittels „umfassender Persönlichkeits- und Bewegungsprofile" auf die Persönlichkeit und Gesinnung des Betroffenen geschlossen werden kann, werde nicht jene Eingriffsintensität erreicht, die den VfGH zu der Annahme der Verfassungswidrigkeit des geltenden § 111 Abs. 2 öStPO bewogen habe.[49]

Diese Argumentation des Entwurfs steht auf wackligen Beinen: Zum einen kommt es nach § 109 Z. 1 lit. a öStPO-Entw. nicht darauf an, ob es sich bei dem Sichergestellten um den „gesamten Datenträger" bzw. „sämtliche Daten" handelt, und auch nicht darauf, ob diese Daten noch nach § 109 Z. 2b öStPO-Entw. „aufbereitet" werden müssen, sondern nur darauf, dass Datenträger bzw. Daten „ausgewertet" werden sollen. Eine Sicherstellung von Daten, die mittels Bild- und Tonaufzeichnungsgeräten aufgenommenen wurden, erfolgt i. d. R. aus Beweisgründen, um die Aufnahmen auf ihren Beweiswert hin zu sichten. Selbst wenn das relevante Bild- oder Videomaterial nur „in Bezug auf einen bestimmten Zeitpunkt" auf seinen Beweiswert gesichtet und analysiert wird, erfolgt dadurch zwangsläufig eine (wenngleich zeitlich begrenzte) „Auswertung" dieser Daten.[50] Insoweit steht § 111 Abs. 2 öStPO-Entw. im Widerspruch zum Wortlaut des § 109 Z. 1 lit. a des Entwurfs, der die Auswertung von Daten aus Beweisgründen gerade nicht den allgemeinen Sicherstellungsregeln unterwerfen will. Zum anderen sieht der vorgeschlagene Wortlaut des § 111 Abs. 2 öStPO-Entw. eine von den Erläuterungen unterstellte Beschränkung der Daten „auf einen bestimmten Zeitpunkt" gar nicht vor, sondern es werden vielmehr (zeitlich unbeschränkt) alle Daten erfasst, „die mittels Bild- und Tonaufzeichnungsgeräten an öffentlichen oder öffentlich zugänglichen Orten aufgenommen wurden". Dementsprechend ist die potentielle Eingriffsintensität auch nicht auf die in den Erläuterun-

[47] 349/ME 27. GP Erläut. 11.
[48] 349/ME 27. GP Erläut. 1, 12 f.
[49] 349/ME 27. GP Erläut. 13; VfGH 14.12.2023, G 352/2021.
[50] So auch treffend die Stellungnahme des *BKA – Verfassungsdienst*, Stellungnahme zum ME eines Ersten Bundesrechtsbereinigungsgesetzes, 14/SN-349/ME, 5.

gen[51] erwähnten besonderen Fälle (Überwachungskameras z. B. in Supermärkten, Banken, öffentlichen Verkehrsmitteln; Fotos aus Bankomatkameras) beschränkt. Auch private Smartphones sind „Bild- und Tonaufzeichnungsgeräte", und „jede Person" ist zur Herausgabe und zur Ermöglichung des Datenzugriffs verpflichtet; „öffentlich zugänglich" sind überdies auch ein Wirtshaus, ein öffentliches Schwimmbad, der Hörsaal einer Universität, eine Mensa, eine öffentliche Bibliothek, ein Kino oder Theater, die Wartebereiche in öffentlichen Krankenhäusern und Arztpraxen. Hier ergeben sich vielfältige und weitreichende Möglichkeiten für Strafverfolgungsorgane, sich abseits spezieller materieller oder formeller Schranken Zugriff auf umfangreiches, personenbezogenes Datenmaterial zu verschaffen. Im Übrigen ist nicht ausgemacht, dass die Sicherstellung und „Sichtung" eines vielleicht mehrstündigen Videomaterials aus Überwachungskameras und privaten Handys, das Menschen bei einer Versammlung, Protestaktion oder sonstigen Aktivitäten zeigt, nicht auch Rückschlüsse auf die Gesinnung und Persönlichkeit der Betreffenden zulässt.[52]

Die Beschlagnahme von Datenträgern und Daten muss nach dem Entwurf (§ 115f Abs. 2) durch die Staatsanwaltschaft auf Grund einer richterlichen Bewilligung angeordnet und von der Kriminalpolizei durchgeführt werden. Anordnung und Bewilligung haben den Beschuldigten, soweit er bekannt ist, und die Tat, derer er verdächtig ist, sowie die Tatsachen zu bezeichnen, aus denen sich ergibt, dass Anordnung und Bewilligung zur Aufklärung der Tat erforderlich und verhältnismäßig sind; darüber hinaus müssen sie die zu beschlagnahmenden Datenkategorien und Dateninhalte umschreiben sowie den von der Beschlagnahme betroffenen Zeitraum angeben (§ 115f Abs. 3 erster Satz öStPO-Entw.). Die Beschlagnahme darf nur für jenen Zeitraum angeordnet werden, der zur Erreichung ihres Zwecks voraussichtlich erforderlich ist (§ 115f Abs. 3 zweiter Satz öStPO-Entw.). Im Übrigen sind die Anforderungen an die Zulässigkeit der Maßnahme gering: Sie scheint aus Beweisgründen erforderlich und bestimmte Tatsachen lassen annehmen, es könnten durch sie Informationen ermittelt werden, die für die Aufklärung einer Straftat wesentlich sind (§ 115f Abs. 1 öStPO-Entw.).

Es genügt demnach, wenn die zu erwartenden Informationen für die Aufklärung irgendeiner Straftat wesentlich sind. Es muss weder eine Tat von Gewicht noch ein besonderer Verdachtsgrad vorliegen, vielmehr reicht schon der Anfangsverdacht irgendeiner Straftat.[53] Der Anfangsverdacht ist der geringste nach dem Gesetz mögliche Verdachtsgrad, für den es ausreicht, dass eine Straftat auch nur möglich er-

---

[51] 349/ME 27. GP Erläut. 13.

[52] Ähnliche Bedenken aufzeigend in Hinblick auf „jede natürliche Person, die bspw. an einer öffentlichen Kundgebung teilnimmt und dabei Bild- und Tonaufzeichnungen mit einem Mobiltelefon macht" in der Stellungnahme des BKA – Verfassungsdienst (Fn. 49), 6.

[53] Zumal die beschlagnahmten Daten nur zu vernichten sind und der in Beschlag genommene Datenträger nur zurückzugeben ist, wenn das OLG einer Beschwerde des Betroffenen stattgibt, weil nicht einmal ein Anfangsverdacht vorliegt (§ 115f Abs. 7 öStPO-Entw. unter Hinweis auf § 89 Abs. 4 öStPO). 349/ME 27. GP Erläut. 17.

scheint.[54] So kann grundsätzlich schon die bloße Möglichkeit einer Bagatelltat zur Beschlagnahme und Auswertung beispielsweise eines Smartphones führen, wenn dies für die Aufklärung der Tat wesentlich erscheint.

Nach dem Erkenntnis des VfGH muss der Gesetzgeber bei der Ausgestaltung der strafrechtlichen Ermittlungsmaßnahme abhängig von der Intensität des Eingriffs einen Ausgleich zwischen dem Strafverfolgungsinteresse und dem Interesse der (verdächtigen oder unverdächtigen) Betroffenen auf Schutz ihrer Grundrechte (hier § 1 DSG, Art. 8 EMRK) vornehmen.[55] Dieser Ausgleich ist, wie schon unter VI.1. dargestellt, durch die Beachtung gewisser Gesichtspunkte zu erzielen.[56] Während die einen die materiellen Voraussetzungen des Eingriffs betreffen,[57] beziehen sich die anderen auf verfahrensrechtliche Schutzmechanismen.[58] Der Gesetzgeber muss beiden Aspekten Rechnung tragen, indem er einerseits die Rechte der Betroffenen im Verfahren durch wirksame Informations-, Kontroll- und Aufsichtsrechte absichert und andererseits den Eingriff nach materiellen Gesichtspunkten begrenzt.[59] Im Entwurf fehlen konkrete materielle Beschränkungen des Eingriffs, obwohl der VfGH einen „Unterschied" gerade darin erblickt, „ob" der Gesetzgeber die Möglichkeit der Sicherstellung von Datenträgern und der Auswertung der darauf (lokal oder extern) gespeicherten Daten „bei einem Anfangsverdacht der Begehung einer Straftat einerseits unabhängig von ihrer Schwere, von dem mit dem Straftatbestand geschützten Rechtsgut oder von dem bei der Begehung einer Straftat typischerweise eingesetzten Datenträger (‚Cyberkriminalität') oder aber andererseits nur bei bestimmten Straftaten vorsieht".[60] Wenn demgegenüber der Entwurf den Eingriff ohne Rücksicht auf die Schwere der Tat, das geschützte Rechtsgut oder die Art der Tatbegehung ermöglicht, ihn also nicht auf „bestimmte Straftaten" beschränkt, könnte der anzustrebende Ausgleich, was materielle Gesichtspunkte angeht, weiterhin nur auf Basis einer allgemeinen Verhältnismäßigkeitsprüfung erfolgen.[61] Entgegen den Erläuterungen[62] geschähe auf diese Weise gerade kein „umfassender Ausgleich" zwischen den Strafverfolgungsinteressen und den durch die Sicherstellung und Auswertung verursachten Grundrechtseingriffen. Und da der VfGH ausdrücklich betont, dass es für den erforderlichen Ausgleich nicht genügt, „dass die im Ermittlungsverfahren befassten Organe bei der Ausübung ihrer Befugnisse den in § 5 öStPO nor-

---

[54] *Bertel*, in: Bertel/Venier, StPO I, 2. Aufl., 2022, § 1 StPO Rn. 1, *Markel*, in: Fuchs/Ratz, WK-StPO, 237. Lfg., September 2015, § 1 StPO Rn. 26.

[55] VfGH 14.12.2023, G 352/2021, Rn. 97.

[56] VfGH 14.12.2023, G 352/2021, Rn. 98 ff.

[57] VfGH 14.12.2023, G 352/2021, Rn. 99.

[58] VfGH 14.12.2023, G 352/2021, Rn. 100 ff.

[59] Siehe auch Stellungnahme *Schwaighofer/Venier*, Stellungnahme zum ME eines Strafprozessrechtsänderungsgesetzes 2024 und zum Initiativantrag 4125/A, 277976/SN, 2.

[60] VfGH 14.12.2023, G 352/2021, Rn. 99.

[61] So aber 349/ME 27. GP Erläut. 16.

[62] 349/ME 27. GP Erläut. 14.

mierten allgemeinen Verhältnismäßigkeitsgrundsatz zu beachten haben",[63] bliebe insoweit die Verfassungswidrigkeit des Gesetzes weiter bestehen.[64]

Wenn für die Durchsuchung einer Wohnung derzeit keine bestimmte Tatschwere verlangt wird, für die Beschlagnahme von Datenträgern und Daten in Zukunft aber schon, so läge darin – entgegen den Erläuterungen[65] – kein Wertungswiderspruch. Im Gegenteil, es wäre ein Wertungswiderspruch, wenn für die Beschlagnahme von Datenträgern und Daten nicht mindestens dieselben Anforderungen an die Tatschwere gestellt werden wie für die Beschlagnahme von Briefen (Vorsatztat mit über einem Jahr Freiheitsstrafdrohung) oder die Auskunft über Daten einer Nachrichtenüberwachung (Vorsatztat mit über einem Jahr, bei Zustimmung des Geräteinhabers mehr als sechs Monate Freiheitsstrafdrohung).[66]

Nach dem Entwurf (§ 115j Abs. 1) dürfen „Ergebnisse einer Auswertung" bei sonstiger Nichtigkeit nur verwendet werden, wenn die Beschlagnahme von Datenträgern und Daten „rechtmäßig" angeordnet und bewilligt wurde. Der Entwurf verweist auf § 115f Abs. 2, der die Notwendigkeit der Anordnung und Bewilligung der Beschlagnahme betont, ein Verweis auf § 115f Abs. 1 des Entwurfs fehlt hingegen, obwohl dort die materielle Zulässigkeit der Maßnahme umschrieben wird. Die Nichtigkeitssanktion sollte aber auch dann eintreten, wenn die Beschlagnahme „nur" nach § 115f Abs. 1 inhaltlich verfehlt ist.

Der Entwurf enthält zur Beschlagnahme von Datenträgern und Daten auch eine Reihe von Verfahrensvorschriften, die hier nicht näher dargestellt werden können und von denen zum gegenwärtigen Zeitpunkt zweifelhaft ist, ob sie in dieser Form Gesetz werden.[67] Besonders kritisiert wird etwa die beabsichtigte organisatorische Trennung von Datenaufbereitung und Datenauswertung.[68] Der Entwurf will den Prozess der Datenaufbereitung (§ 115h öStPO-Entw.) in die Hände einer eigenständigen polizeilichen Forensik-Einheit legen und die eigentlich ermittelnde Kriminalpolizei und vor allem die Staatsanwaltschaft auf den Prozess der Datenauswertung (§ 115i öStPO-Entw.) beschränken. Dem Staatsanwalt als Leiter des Ermittlungsverfahrens wird man jedoch nicht das Recht absprechen können, zumindest formal auch den Prozess der Datenaufbereitung zu leiten, entsprechend den Regeln, die gegenwärtig § 138 Abs. 4 öStPO bei der Überwachung von Nachrichten vorgibt.[69] Hier ist noch nicht das letzte Wort gesprochen.

---

[63] VfGH 14.12.2023, G 352/2021, Rn. 89, 92.

[64] Stellungnahme *Schwaighofer/Venier* (Fn. 58), 3.

[65] 349/ME 27. GP Erläut. 14 f.

[66] Dazu oben unter IV.

[67] Die Justizministerin hat eine Änderung des Entwurfs angekündigt.

[68] Federführend *Vereinigung der österreichischen Staatsanwältinnen und Staatsanwälte*, Stellungnahme zum ME eines Ersten Bundesrechtsbereinigungsgesetzes, 2/SN-349/ME, 3 ff. Gegenteilig allerdings *Österreichischer Rechtsanwaltskammertag*, Stellungnahme zum ME eines Strafprozessrechtsänderungsgesetzes 2024, 25/SN-349/ME, 5.

[69] Stellungnahme *Schwaighofer/Venier* (Fn. 58), 4.

## VII. Resümee

Im Lichte der Judikatur des VfGH (VI.1.) und in Anlehnung an die Regeln der Überwachung von Nachrichten (IV.) sollte das Gesetz zum Schutz der Rechte der Betroffenen zumindest folgenden Anforderungen genügen:[70]

In materieller Hinsicht sollte die Sicherstellung von digitalen Endgeräten (z. B. Smartphones, Laptops, PC) und die Auswertung der darauf oder an anderen Orten (z. B. Cloud) gespeicherten Kommunikationsdaten nur zur Aufklärung einer Vorsatztat zulässig sein, die mit mehr als einem Jahr Freiheitsstrafe bedroht ist. Formell sind jedenfalls eine begründete Anordnung des Staatsanwalts und eine begründete richterliche Bewilligung erforderlich. Stampiglien-Beschlüsse, bei denen der Richter anstelle einer eigenen Begründung auf die Begründung in der Anordnung des Staatsanwalts verweist, sollten endlich und nicht nur hier der Vergangenheit angehören.[71]

In der Folge sollte die Auswertung der Daten lückenlos dokumentiert und nur für das Verfahren erhebliche und verwertbare Daten zum Akt genommen werden (vgl. § 138 Abs. 4 öStPO). Die Betroffenen sollten zeitnah Einsicht in das von der Auswertung betroffene Datenmaterial erhalten und wie bei einer Nachrichtenüberwachung oder Datenauskunft beantragen können, unerhebliche oder unverwertbare Ergebnisse auszuscheiden (vgl. § 139 Abs. 1, 2, 4 öStPO). Die Ergebnisse einer formell oder materiell nicht rechtmäßigen Datenauswertung sollten wie jene einer nicht rechtmäßigen Nachrichtenüberwachung oder Datenauskunft bei sonstiger Nichtigkeit nicht als Beweismittel verwendet werden dürfen (vgl. § 140 Abs. 1 Z. 2, 4 öStPO). Der Entwurf eines Strafprozessrechtsänderungsgesetzes 2024 (VI.2.) bleibt jedenfalls in der Frage der materiellen Zulässigkeit der Datensicherstellung und Datenauswertung hinter diesen Ansprüchen zurück.[72]

---

[70] Vgl. auch *Venier/Tipold*, Strafprozessrecht, 16. Aufl., 2024, Vorwort.

[71] *Bertel*, in: Bertel/Venier, StPO I, 2. Aufl., 2022, § 86 StPO Rn. 3 ff.; *Pilnacek*, ZWF 2023, 50 (57).

[72] Nicht mehr berücksichtigt werden konnte das erst bei Drucklegung im Nationalrat beschlossene Strafprozessrechtsänderungsgesetz 2024. Es setzt – von gewissen Änderungen abgesehen (z. B. der Staatsanwalt leitet nun auch die Datenaufbereitung) – lediglich die Überlegungen des Ministerialentwurfs um.

# Die Europäische Staatsanwaltschaft

## Was kann sie zur grenzüberschreitenden Strafverfolgung beitragen?

*Konrad Kmetic*



## I. Grundlegendes

Die Europäische Staatsanwaltschaft (EUStA) ist eine der innovativsten Neuerungen im Bereich der justiziellen Zusammenarbeit der Europäischen Union (EU) in den letzten Jahren. Sie wurde geschaffen, um die effektive Bekämpfung von Straftaten zu gewährleisten, die zum Nachteil der finanziellen Interessen der EU begangen werden. In diesem Beitrag soll die Entstehungsgeschichte der EUStA untersucht, ihre Organisationsstruktur analysiert und ihre Funktionen sowie ihre potenziellen Auswirkungen auf die europäische Rechtslandschaft, insbesondere ihr neuartiges System der grenzüberschreitenden Zusammenarbeit nach der Art einer „internen Rechtshilfe“, diskutiert werden. Schließlich soll ein erstes Resümee darüber gezogen werden, inwieweit sich die Erwartungen an den „neuen Spieler auf dem Feld des europäischen Strafrechts“ erfüllt haben, um abschließend das Umfeld der „Mitspieler“ auf diesem Feld darzustellen.

Die Schaffung der EUStA hat potenziell weitreichende Auswirkungen auf die europäische Rechtslandschaft. Sie trägt zur Stärkung der Rechtsdurchsetzung bei, indem sie die Strafverfolgung von Straftaten gegen die finanziellen Interessen der EU auf eine neue Grundlage stellt. Gleichzeitig wirft die EUStA Fragen im Hinblick auf die Zuständigkeiten der EU und der Mitgliedstaaten für das nach wie vor von den nationalen Rechten dominierte Feld der Strafrechtspflege auf, was sich ganz konkret in der Frage der Zuständigkeit der EUStA und des für sie relevanten Verfahrensrech-

tes ausdrückt. Maßstab für das Gelingen des Vorhabens sind auch die Rechte der Beschuldigten, die insbesondere durch „umfassende Verfahrensgarantien auf der Grundlage des geltenden EU-Rechts und des nationalen Rechts gewährleistet" werden sollen.[1] Eine besondere Rolle kommt dabei nach Ansicht der Kommission den in der Charta der Grundrechte der Europäischen Union verankerten Rechten, einschließlich des Rechts auf ein faires Verfahren und des Rechts auf Verteidigung, zu.

## II. Rechtliche Grundlagen und Organisation der EUStA

Die Idee einer europäischen Strafverfolgungsbehörde wurde erstmals in den 1990er Jahren diskutiert, als die EU begann, Maßnahmen zur Bekämpfung von Betrug und anderen strafbaren Handlungen gegen ihre finanziellen Interessen zu ergreifen. Der Vertrag von Lissabon von 2009 legte schließlich den rechtlichen Rahmen für die Schaffung der EUStA fest. Dieser Vertrag stärkte die Befugnisse der EU im Bereich der justiziellen Zusammenarbeit und ermöglichte die Einführung neuer Institutionen wie die der EUStA.[2]

Die Hauptaufgabe der EUStA besteht darin, Straftaten zu verfolgen, die zum Nachteil der finanziellen Interessen der EU begangen werden. Dazu gehören Fälle von Betrug, Korruption, Geldwäsche und andere schwere Straftaten. Die EUStA hat das Recht, Ermittlungen durchzuführen, Anklagen zu erheben und vor Gericht zu vertreten. Laut Kommission soll sie „als zentrale, alle Mitgliedstaaten übergreifende Behörde fungieren und europäische und nationale Strafverfolgung in den teilnehmenden Mitgliedstaaten in reibungsloser und effizienter Zusammenarbeit miteinander kombinieren".[3]

An der Wiege der EUStA standen zwei europarechtliche Dokumente, beide – ob Zufall oder nicht – aus dem Jahr 2017. Beim ersteren handelt es sich um die Verordnung (EU) 2017/1939 des Rates vom 12. Oktober 2017 zur Durchführung einer verstärkten Zusammenarbeit zur Errichtung der Europäischen Staatsanwaltschaft (EUStA) – auch kurz EUStA-VO.[4] Als VO ist dieses Dokument unmittelbar anwendbar. Subsidiär dazu ergingen aber auch nationale (Verfahrens-)Vorschriften. So fin-

---

[1] *Europäische Kommission*, Factsheet zur Europäischen Staatsanwaltschaft, abrufbar unter https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/networks-and-bodies-supporting-judicial-cooperation/european-public-prosecutors-office-eppo_de#aufgaben (Abrufdatum: 31.5.2024).

[2] Vertrag von Lissabon zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft, unterzeichnet in Lissabon am 13. Dezember 2007, ABl. C 306/1 vom 17.12.2007.

[3] *Europäische Kommission*, Factsheet zur Europäischen Staatsanwaltschaft, abrufbar unter https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/networks-and-bodie-supporting-judicial-cooperation/european-public-prosecutors-office-eppo_de#aufgaben (Abrufdatum: 31.5.2024).

[4] ABl. L 283/1 vom 31.10.2017: Folgende Art. und ErwGr. ohne nähere Bezeichnung beziehen sich auf diese Verordnung.

den sich in der VO zahlreiche Verweise auf nationales Recht, wo es zur näheren Ausgestaltung einer nationalstaatlichen „Umsetzung" bedurfte.

Die zentrale Umsetzung in Österreich erfolgte im Zuge des Strafrechtlichen EU-Anpassungsgesetzes – StrEU-AG 2021,[5] welches auch das Bundesgesetz zur Durchführung der Europäischen Staatsanwaltschaft – EUStA-DG enthält.[6] In Kraft getreten ist dieses am 29.5.2021. Dazu ergangen ist auch der Einführungserlass des BMJ vom 29.10.2021, GZ: 2021 0.585.850 (S753.000/IV.2).

Dieses erste Regelwerk, obwohl nicht nur als das namensgebende Dokument die zentrale Bestimmung der EUStA, wäre ohne das zweite jedoch nicht denkbar. Dabei handelt es sich um die Richtlinie (EU) 2017/1371 des Europäischen Parlaments und des Rates vom 5. Juli 2017 über die strafrechtliche Bekämpfung von gegen die finanziellen Interessen der Union gerichtetem Betrug, die sogenannte „PIF-Richtlinie".[7] Diese umschreibt die materielle Zuständigkeit der EUStA, da Art. 22 EUStA-VO – die zentrale Kompetenzbestimmung – inhaltlich darauf verweist. Die PIF-Richtlinie beschreibt im Wesentlichen Straftaten zum Nachteil des EU-Haushalts und damit in Zusammenhang stehende Taten. Gefordert wird von sämtlichen EU-Mitgliedstaaten[8] eine Angleichung des materiellen Strafrechts der Mitgliedstaaten betreffend diese „PIF-Delikte".

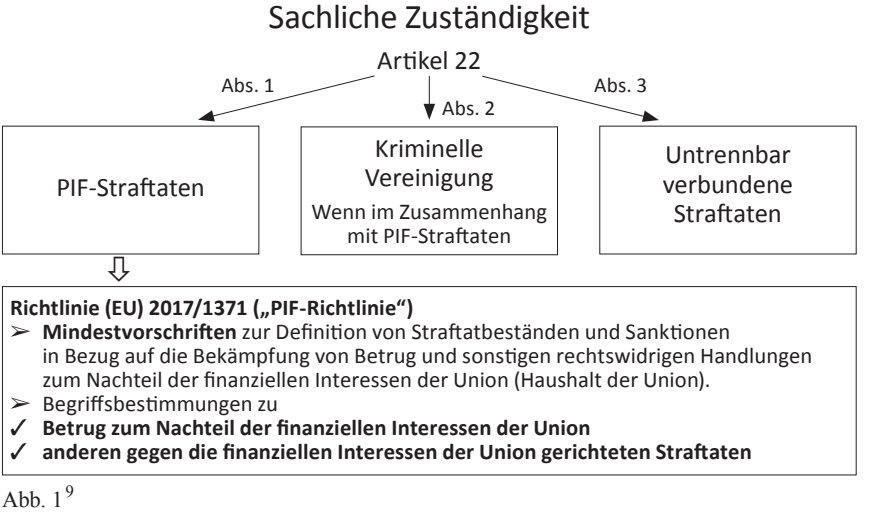


Abb. 1[9]

[5] BGBl. I 94/2021.

[6] Daneben enthält es v. a. auch die Bestimmungen zur Durchführung der Verordnung (EU) 2018/1805 vom 14. November 2018 über die gegenseitige Anerkennung von Sicherstellungs- und Einziehungsentscheidungen, ABl. L 303/1 vom 28.11.2018.

[7] PIF-RL, ABl. L 198/29 vom 28.7.2017.

[8] Ausnahme ist nunmehr lediglich Dänemark, welches weiterhin den Vorgänger, das PIF-Übereinkommen, anwendet: *Rat der Europäischen Union*, Gutachten des juristischen Dienstes, Brüssel, den 22. Oktober 2012, 15309/12, 8.

[9] *ERA*, Zuständigkeiten der EUStA: Zusammenarbeit mit der EUStA auf dezentraler Ebene, Schulungsmaterial für Staatsanwälte und Ermittlungsrichter.

Als Richtlinie musste sie ins nationale Recht der Mitgliedstaaten umgesetzt werden, Frist dafür war der 6.7.2019.[10] In Österreich erfolgte dies, spät aber doch, einerseits im Zuge des EU-Finanz-Anpassungsgesetzes 2019 (EU-FinAnpG 2019)[11] zum 23.7. 2019, andererseits durch das „Bundesgesetz, mit dem das Strafgesetzbuch, das Gesetz über das Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung und die Strafprozessordnung 1975 zur Umsetzung der Richtlinie über die strafrechtliche Bekämpfung von gegen die finanziellen Interessen der Union gerichteten Betrug geändert wurden“[12] zum 28.12.2019.

Die EUStA hat eine komplexe Struktur, die aus einem zentralen und einem dezentralen Bereich besteht. Auf zentraler Ebene befindet sich das Kollegium, das aus der Europäischen Generalstaatsanwältin und ihren Stellvertretern sowie den Europäischen Staatsanwälten der teilnehmenden Mitgliedstaaten besteht. Das Kollegium ist für die allgemeine strategische Ausrichtung und die Überwachung der Tätigkeiten der EUStA verantwortlich.[13]

Auf dezentraler Ebene agieren die Europäischen Delegierten Staatsanwälte, die in den jeweiligen Mitgliedstaaten angesiedelt sind. Sie führen die Ermittlungen und Strafverfolgungen vor Ort durch, jedoch unter der Aufsicht des zentralen Büros der EUStA. Diese Struktur soll es der EUStA ermöglichen, effizient und kohärent über die Grenzen der Mitgliedstaaten hinweg zu arbeiten, gleichzeitig die nationalen Rechtssysteme zu respektieren, aber von deren Strafverfolgungsbehörden unabhängig zu agieren.[14]

Derzeit nehmen 22 EU-Mitgliedstaaten an der EUStA teil. Diese Staaten sind Belgien, Bulgarien, Deutschland, Estland, Finnland, Frankreich, Griechenland, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, die Niederlande, Österreich, Portugal, Rumänien, die Slowakei, Slowenien, Spanien, die Tschechische Republik und Zypern.[15]

---

[10] Art. 17 PIF-RL.

[11] BGBl. I 2019/62.

[12] BGBl. I 2019/111.

[13] *European Public Prosecutor‘s Office*, abrufbar unter https://www.eppo.europa.eu/en/about/structure-and-characteristics (Abrufdatum: 31.5.2024).

[14] *European Public Prosecutor‘s Office*, abrufbar unter https://www.eppo.europa.eu/en/about/structure-and-characteristics (Abrufdatum: 31.5.2024).

[15] *Europäische Staatsanwaltschaft*, Liste der teilnehmenden Mitgliedstaaten, abrufbar unter https://www.eppo.europa.eu/en/about/members (Abrufdatum: 31.5.2024).

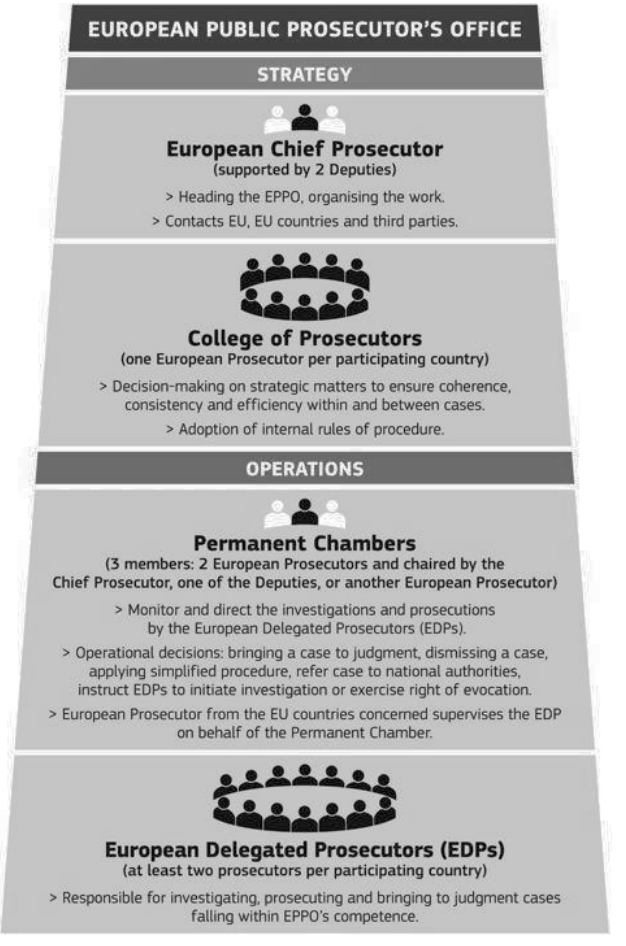


Abb. 2 [16]

## III. Arbeitsweise der EUStA

Die EUStA hat weitreichende Befugnisse in Bezug auf Ermittlungs- und Strafverfolgungsverfahren. Sobald ein Fall an die EUStA verwiesen wird oder sie von sich aus ein Verfahren einleitet, kann sie eine Vielzahl von Ermittlungsmaßnahmen ergrei-

[16] *Europäische Kommission*, Factsheet zur Europäischen Staatsanwaltschaft, abrufbar unter https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/networks-and-bodies-supporting-judicial-cooperation/european-public-prosecutors-office-eppo_de#aufgaben (Abrufdatum: 31.5.2024).

fen. Dazu gehören Durchsuchungen, Beschlagnahmungen, die Überwachung von Kommunikationsmitteln und die Einziehung von Vermögenswerten. Diese Maßnahmen müssen den jeweiligen nationalen Vorschriften entsprechen und werden durch innerstaatliche Polizei- und Finanzorgane durchgeführt.[17]

Die EUStA erhebt schließlich direkt vor den nationalen Gerichten der Mitgliedstaaten Anklage. Dies stellt eine erhebliche Neuerung dar, da bisherige EU-Behörden wie OLAF (das Europäische Amt für Betrugsbekämpfung) keine direkten Strafverfolgungsbefugnisse hatten, sondern lediglich Empfehlungen aussprechen konnten. Die Delegierten Staatsanwälte der EUStA sind befugt, vor den nationalen Gerichten aufzutreten und dort die Interessen der EU zu vertreten.[18]

Gerade was die grenzüberschreitenden Ermittlungen in Strafsachen zwischen den am EUStA-Projekt teilnehmenden Mitgliedstaaten anbelangt, sollte Art. 31 EUStA-VO diese auf völlig neue Beine stellen. Diese Bestimmung sieht vor, dass Ermittlungsmaßnahmen in mehreren Mitgliedstaaten durchgeführt werden können, wobei die Zuständigkeit und Koordination zwischen dem betrauten Delegierten Europäischen Staatsanwalt (betrDEStA) und dem unterstützenden Delegierten Europäischen Staatsanwalt (untDEStA) aufgeteilt wird. Diese Struktur zielt darauf ab, die Effizienz und Kohärenz der Strafverfolgung innerhalb der EU zu erhöhen, indem sie die bestehenden Mechanismen der traditionellen Rechtshilfe überwindet und ein System der gegenseitigen Anerkennung schafft. Dabei stellt Art. 31 EUStA-VO sicher, dass der betrDEStA die federführende Rolle übernimmt und über die Notwendigkeit und Art der Maßnahmen entscheidet, die in einem anderen Mitgliedstaat durchgeführt werden sollen. Die EUStA führt ein duales System ein, bei dem der betrDEStA die Hauptverantwortung für das Ermittlungsverfahren trägt und die zu treffenden Maßnahmen bestimmt. Diese Maßnahmen werden dann dem untDEStA zur Durchführung zugewiesen, der sie nach den nationalen Rechtsvorschriften seines Mitgliedstaats umsetzt. Diese Aufgabenteilung spiegelt den Grundgedanken eines „*single office*" wider, bei dem die verschiedenen europäischen Staatsanwälte als Teil einer einheitlichen Behörde agieren sollen.

Art. 31 Abs. 3 der Verordnung legt fest, dass wenn richterliche Genehmigungen für bestimmte Maßnahmen erforderlich sind, die jeweilige rechtliche Grundlage von dem Mitgliedstaat abhängt, in dem die Maßnahme durchgeführt wird. Diese Regelung kann jedoch zu Komplikationen führen. Ein prägnantes Beispiel für die praktischen Herausforderungen der grenzüberschreitenden Zusammenarbeit bildet die Rechtssache C-281/22 vor dem Europäischen Gerichtshof (EuGH) ab. Hier wurde die Frage aufgeworfen, wie die richterliche Genehmigung für Hausdurchsuchungen zu handhaben ist, wenn sowohl im Staat des betrDEStA als auch im Staat des untDEStA

[17] *Europäische Kommission*, Ermittlungsbefugnisse der EUStA, abrufbar unter https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/networks-and-bodies-supporting-judicial-cooperation/european-public-prosecutors-office-eppo_de (Abrufdatum: 31.5.2024).

[18] *Europäisches Amt für Betrugsbekämpfung (OLAF)*, Vergleich der EUStA mit OLAF, abrufbar unter https://ec.europa.eu/anti-fraud/about-us_en (Abrufdatum: 31.5.2024).

richterliche Genehmigungen erforderlich sind. Die unterschiedlichen Interpretationen der Verordnung zeigen, dass sowohl die Wortlautinterpretation als auch die teleologische Auslegung verschiedene Ergebnisse zulassen. Während die deutsche und österreichische Regierung eine umfassende richterliche Kontrolle befürworteten, argumentierten die EUStA, die Kommission und andere Regierungen für eine Beschränkung auf formelle Aspekte der Durchführung der Maßnahmen.

Die Generalanwältin des EuGH betonte in ihren Schlussanträgen die Notwendigkeit einer Zusammenschau der unterschiedlichen Auslegungsregeln und hob hervor, dass die praktische Wirksamkeit der Vorschriften gewahrt bleiben müsse. Sie schlug eine Lösung vor, die sowohl die materiellen Voraussetzungen der Maßnahme durch den betrDEStA als auch die formellen Anforderungen durch den untDEStA berücksichtigt.[19] Am 21.12.2023 entschied der Gerichtshof in dieser Rechtssache.[20] Dabei folgte er nur im ersten Urteilspunkt den Schlussfolgerungen der Generalanwältin: Die Kontrolle des Gerichts im Land des untDEStA hat sich nur auf die Gesichtspunkte der Vollstreckung, nicht aber auf die inhaltlichen Punkte („Begründung und Anordnung der Maßnahme") zu beziehen. Im Fall „schwerwiegender Eingriffe" in die durch die Charta der Grundrechte garantierten Rechte bedarf es *auch* im Land des betrDEStA einer gerichtlichen Bewilligung der Maßnahme („vorherige gerichtliche Kontrolle").

## IV. Erwartung und Erfüllung

Die EUStA ist angetreten, bedeutende finanzielle Schäden für die Europäische Union zu verhindern und somit einen erheblichen Mehrwert zu schaffen. Schätzungen dazu legten die Messlatte durchaus hoch: So lag der geschätzte Ausfall an Mehrwertsteuer durch Betrug bei 60 Milliarden Euro pro Jahr sowie der geschätzte Schaden durch Betrug zum Nachteil der EU bei 500 Millionen Euro pro Jahr. Lassen sich die durch diese Beträge ausgedrückten Erwartungen durch die statistischen Ergebnisse der EUStA bislang als erfüllt ansehen? Für das Jahr 2022 ergeben sich aus den vorliegenden Daten folgende Ergebnisse:[21] Über 1100 Ermittlungsverfahren wurden eingeleitet, darin dem Verdacht nachgegangen, dass durch Tathandlungen ein Schaden von insgesamt rund 14 Milliarden Euro verursacht worden war. Davon wurde ein „Gegenwert" von ca. 360 Millionen Euro auch gesichert. Nach einem Jahr operativer Tätigkeit lagen auch 87 Anklagen und 20 Verurteilungen vor.[22]

---

[19] Schlussanträge der Generalanwältin *Tamara Capeta* v. 22.6.2023 – Rs. C-281/22 (G. K. u. a.), abrufbar unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62022CC0281 (Abrufdatum: 31.5.2024).

[20] EuGH, Urt. v. 21.12.2023 – Rs. C-281/22 (G. K. u. a.).

[21] EUStA-Jahresbericht 2022, abrufbar unter https://www.eppo.europa.eu/sites/default/files/2023-02/EPPO_2022_Annual_Report_EN_WEB.pdf (Abrufdatum 31.5.2024).

[22] Abrufbar unter https://www.eppo.europa.eu/en/media/news/annual-report-2022-eppo-puts-spotlight-revenue-fraud (Abrufdatum 31.5.2024).


Abb. 3[23]

## V. Die EUStA und ihre „Partner"

Die EUStA agiert in einem komplexen Netzwerk internationaler Zusammenarbeit. Die rechtliche Grundlage für die Zusammenarbeit mit Nicht-EU-Staaten und nicht teilnehmenden EU-Mitgliedstaaten basiert auf dem Prinzip der Gegenseitigkeit sowie auf internationalen Vereinbarungen. Die EUStA hat aber auch Arbeitsvereinbarungen mit verschiedenen internationalen Partnern getroffen, um die Kooperation zu erleichtern und die Effizienz ihrer Ermittlungen zu steigern.[24] Ein besonderer Stellenwert kommt dabei den „Partnern auf EU-Ebene", den sogenannten *IBOA*[25] zu.

[23] EUStA-Jahresbericht 2022, 12 f., abrufbar unter https://www.eppo.europa.eu/sites/default/files/2023-02/EPPO_2022_Annual_Report_EN_WEB.pdf (Abrufdatum: 31.5.2024).

[24] Die Grundlage dafür bildet Kapitel X der EUStA-VO: Bestimmungen über die Beziehungen der EUStA zu ihren Partnern, Art. 99–105 und Art. 66–67 der EUStA-Verfahrensordnung (*Internal Rules of Prozedure*, IRP).

[25] IBOA für „*institutions, bodies, offices and agencies of the EU*".

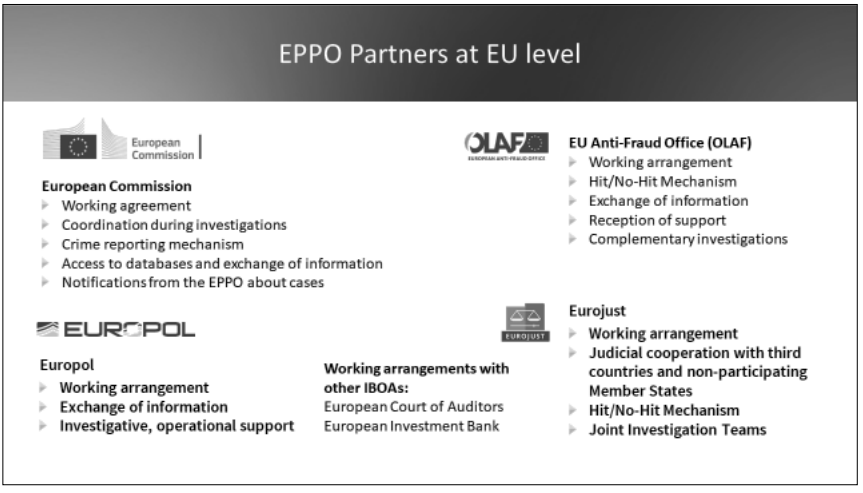


Abb. 4[26]

## VI. Resümee

Die Europäische Staatsanwaltschaft wurde als weiteres, vielleicht wichtigstes Instrument zur Bekämpfung von Straftaten gegen die finanziellen Interessen der EU geschaffen. Ihre Entstehung, Struktur und Funktionen sind eng mit der Entwicklung der europäischen justiziellen Zusammenarbeit verbunden. Die EUStA hat zweifellos den Anspruch, die Effektivität der Strafverfolgung in diesem Bereich zu verbessern, wirft jedoch auch komplexe rechtliche und institutionelle Fragen auf, die wohl weiterhin sorgfältig analysiert, beobachtet und diskutiert werden müssen. Dabei wird der EuGH mit weiteren Entscheidungen letztlich eine entscheidende Rolle spielen. Ob die EUStA „ihr Geld wert ist", also den doch erheblichen Aufwand, der für ihre Schaffung und ihren Betrieb erforderlich ist, rechtfertigt, ist letztlich eine politische Entscheidung der Mitgliedstaaten. Viel wird von der für die nächsten Jahre angesetzten Evaluierung abhängen. Die Behörde arbeitet derweil daran, den Beweis für ihr Funktionieren bestmöglich zu liefern und legt alljährlich darüber in ihrem „*Annual Report*" Zeugnis ab.

[26] EUStA-Jahresbericht 2022, abrufbar unter https://www.eppo.europa.eu/sites/default/files/2023-02/EPPO_2022_Annual_Report_EN_WEB.pdf, 94 (Abrufdatum: 31.5.2024).

# Bankenaufsicht in Europa, Sanktionen und Maßnahmen[1]

*Günther Hauss*



Vorweg kann zusammenfassend festgehalten werden, dass die im Rahmen der Ringvorlesung zu erörternde Fragestellung, ob Recht ein Instrument zur Förderung der Realisierung gemeinsamer Interessen im internationalen Kontext ist, innerhalb der Euroländer[2] in der Bankenaufsicht anhand des Beispiels des einheitlichen Bankenaufsichtsmechanismus (*Single Supervisory Mechanism* „SSM“) positiv beantwortet

[1] Der Inhalt dieses Beitrages spiegelt die persönliche Meinung des Vortragenden wider und enthält keine rechtsverbindlichen Aussagen oder Auslegungen der Europäischen Zentralbank.

[2] Der Begriff Euroländer bezeichnet in diesem Artikel jenen Raum, in welchem die Mitgliedsländer der Europäischen Union den Euro als gemeinsame Währung führen, auch beschrieben als Eurozone oder Euroraum.

werden kann. Durch die direkte Beaufsichtigung von bedeutenden Kreditinstituten durch die Europäische Zentralbank (EZB) wird insbesondere das Interesse einer einheitlichen Überwachung von Aufsichtsanforderungen und deren Auslegung realisiert, dadurch Rechtssicherheit geschaffen und auch ein Beitrag zur Stabilität der Finanzmärkte geleistet, da Risiken auf supranationaler Ebene identifiziert, beobachtet und adressiert werden können. Da auch Sanktionsinstrumente und Durchsetzungsmaßnahmen von den Kompetenzen der EZB im Rahmen des SSM erfasst sind, findet auch hier eine einheitliche Auslegung, wann ein Verstoß gegeben ist, und eine konsistente Reaktion durch die Anwendung der Sanktionsinstrumente und Durchsetzungsmaßnahmen durch die EZB statt.

## I. Einleitung

Nach einer allgemeinen Einleitung zur europäischen Bankenaufsicht, welche ein grundsätzliches Verständnis für den Aufbau und die Entwicklung derselben schaffen soll, wird anschließend der SSM und die Rolle der EZB detaillierter, aber in gebotener Kürze umrissen, um zunächst die gemeinsamen Interessen, welche durch diesen verwirklicht werden, zu illustrieren. In Folge werden anhand von Fallbeispielen Sanktionsinstrumente und Durchsetzungsmaßnahmen der EZB im Rahmen des SSM erläutert, um auch hier die Verwirklichung von gemeinsamen Interessen durch internationales Recht in Form des EU-Rechts zu beleuchten.

## II. Europäische Bankenaufsicht zur Verwirklichung gemeinsamer Interessen

Kreditinstitute haben eine Vielzahl an rechtlichen Bestimmungen zu befolgen, die unter anderem die Finanzstabilität insgesamt und die Kunden schützen sollen. Die Einhaltung dieser Bestimmungen bedarf einer Kontrolle, einer Aufsicht. Sowohl die rechtlichen Bestimmungen, welche einzuhalten sind, als auch die Struktur der Aufsicht über Kreditinstitute unterlag innerhalb der Europäischen Union in den letzten 20 bis 30 Jahren einer starken Veränderung. Im Rahmen der Aufsicht über Kreditinstitute innerhalb der Europäischen Union markiert der Einheitliche Bankenaufsichtsmechanismus, der *Single Supervisory Mechanism* (SSM) als Teil der Europäischen Bankenunion die bisher größte Veränderung.

### *1. Aufsicht vor 2014 und Schaffung des Einheitlichen Aufsichtsmechanismus*

Der SSM versieht seit dem 4.11.2014 seinen Dienst und ist die konsequente Weiterentwicklung von vorangegangen Strukturen im bankaufsichtlichen Bereich, die bereits unter dem Eindruck und als notwendige Antwort auf die Finanzkrise in den Jahren 2007 bis 2009 angestoßen wurde.

Besonders hervorzuheben ist der Bericht der *de Larosière*-Expertengruppe, die von der EU-Kommission im Jahr 2008 zur Erstellung von Empfehlungen für künftige Finanzregulierung und Finanzaufsicht eingesetzt wurde.[3] Der Bericht stellte im Wesentlichen fest, dass das europäische Regelwerk fragmentiert ist, sowohl im Hinblick auf die zu befolgenden Bestimmungen und die Aufsichtsstrukturen als auch im Hinblick auf Krisenmechanismen. Die Empfehlungen des Berichts berücksichtigend[4] wurde das Europäische Finanzaufsichtssystem, das *European System of Financial Supervision* (ESFS), geschaffen, das ab 1.1.2011 tätig wurde und mikroprudenzielle und makroprudenzielle Aufsicht kombiniert. Im Rahmen des ESFS wurden die Europäische Bankenaufsichtsbehörde, *European Banking Authority* (EBA), die Europäische Wertpapier- und Marktaufsichtsbehörde, *European Securities and Markets Authority* (ESMA), und die Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung, *European Insurance and Occupational Pensions Authority* (EIOPA), sowie der Europäische Ausschuss für Systemrisiken, *European System Risk Board* (ESRB), ins Leben gerufen.[5] Sie sind gemeinsam mit den nationalen Aufsichtsbehörden Teil des ESFS und sollen eine einheitliche und angemessene Finanzaufsicht in der EU und eine weitergehende Harmonisierung und kohärente Auslegung von Recht gewährleisten.[6] Die EBA, welche als Teil des ESFS seit 1.1.2011 besteht, übernahm die Aufgaben des Ausschusses der europäischen Bankaufsichtsbehörden, *Committee of European Banking Supervisors* (CEBS), und wurde mit weiteren Kompetenzen ausgestattet, um eine Harmonisierung von Aufsichtsverfahren und deren Ergebnisse im Bankenbereich zu gewährleis-

---

[3] Report of the High-Level Group on Financial Supervision in the EU chaired by de Larosière, 2009, abrufbar unter https://ec.europa.eu/economy_finance/publications/pages/publication14527_en.pdf (Abrufdatum: 25.7.2024).

[4] Siehe hierzu unter anderem Verordnung (EU) Nr. 1092/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 über die Finanzaufsicht der Europäischen Union auf Makroebene und zur Errichtung eines Europäischen Ausschusses für Systemrisiken, ABl. L 331/1 vom 15.12.2010, ErwGr. 4 bis 11, 13 bis 15.

[5] Verordnung (EU) Nr. 1092/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 über die Finanzaufsicht der Europäischen Union auf Makroebene und zur Errichtung eines Europäischen Ausschusses für Systemrisiken, ABl. L 331/1 vom 15.12.2010; Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/78/EG der Kommission, ABl. L 331/12 vom 15.12.2010; Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/79/EG der Kommission, ABl. L 331/48 vom 15.12.2010; Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde), zur Änderung des Beschlusses Nr. 7162009/EG und zur Aufhebung des Beschlusses 2009/77/EG der Kommission, ABl. L 331/84 vom 15.12.2010.

[6] Vgl. Verordnung (EU) Nr. 1093/2010, Erwägungsgrund 9.

ten.[7] So wurde ihr die Aufgabe übertragen, in den Fällen, in denen es ein in Art. 1 Abs. 2 der Verordnung (EU) Nr. 1093/2010 genannter Rechtsakt vorsieht, technische Regulierungsstandards, auch *Regulatory Technical Standards* (RTS) gem. Art. 10, und technische Durchführungsstandards, auch *Implementing Technical Standards* (ITS) gem. Art. 15 der Verordnung Nr. 1093/2010, auszuarbeiten, welche schließlich von der Kommission erlassen werden.[8] Neben der Ausarbeitung von Leitlinien und Empfehlungen, der Abgabe von Meinungen und Warnungen, Ausarbeitung von Antworten auf Fragestellungen, der Erarbeitung von gemeinsamen Methoden, z. B. für die Durchführung von Stresstests zur Bewertung der Widerstandsfähigkeit von Finanzinstituten bei unterschiedlichen Marktentwicklungen, wurde die EBA für speziell gelagerte Fälle auch mit der Möglichkeit ausgestattet, gegenüber einzelnen Instituten Bescheide zu erlassen, z. B. um neutrale Wettbewerbsbedingungen auf dem Markt aufrechtzuerhalten oder wiederherzustellen oder das ordnungsgemäße Funktionieren und die Integrität des Finanzsystems zu gewährleisten.[9] Trotz weitergehender Kompetenzen der EBA im Vergleich zum CEBS fand keine Übertragung der laufenden Aufsicht über Institute statt. Diese oblag weiterhin auf nationaler Ebene den nationalen Aufsichtsbehörden. Insbesondere das Risiko von unterschiedlichen Interpretationen von an sich harmonisiertem Recht im Euroraum und in der EU blieb somit bestehen. Um diesen Aspekt zu adressieren und grenzüberschreitend tätige Bankengruppen gleichmäßig und ohne sich widersprechende Entscheidungen zu beaufsichtigen, somit auch einer Aufsichtsarbitrage entgegenzuwirken, um Finanzstabilität im Euro-Währungsgebiet weiter zu stärken, komplexe und verbundene Märkte und Institute besser überblicken zu können sowie Risiken rechtzeitig zu erkennen, denen international tätige Institute ausgesetzt sind, wurde schlussendlich das Konzept der überwiegenden Koordinierung von Aufsichtsbehörden auf europäischer Ebene hin zu einer einheitlichen, direkten und laufenden Aufsicht auf Basis des vereinheitlichten europäischen Regelwerks weiterentwickelt.[10] Es wurde sohin der einheitliche Aufsichtsmechanismus, der bereits mehrfach erwähnte *Single Supervisory Mechanism* (SSM) geschaffen. Mit der Verordnung (EU) Nr. 1024/2013 (SSM-

---

[7] Das *Committee of European Banking Supervisors* (CEBS) wurde 2004 von der Europäischen Kommission als unabhängiges Gremium aufgesetzt. Die Aufgaben umfassten die EU-Kommission zu beraten, eine konsistente Implementierung von EU-Richtlinien sicherzustellen, einheitliche Standards durch Richtlinien, Empfehlungen zu schaffen, den Austausch zwischen nationalen Behörden zu verbessern und einheitliche Meldesysteme zu schaffen. Siehe Beschluss der Kommission vom 23. Januar 2009 zur Einsetzung des Ausschusses der europäischen Bankaufsichtsbehörden (2009/78/EG), ABl. L 25/23 vom 29.1.2009.

[8] Siehe z. B. Durchführungsverordnung (EU) 2021/451 der Kommission vom 17. Dezember 2020 zur Festlegung technischer Durchführungsstandards für die Anwendung der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates auf die aufsichtlichen Meldungen der Institute und zur Aufhebung der Durchführungsverordnung (EU) Nr. 680/2014, ABl. L 97/1 vom 19.3.2021.

[9] Siehe hierzu Art. 17 Verordnung (EU) Nr. 1093/2010, vgl. auch Erwägungsgrund 12.

[10] Siehe hierzu auch z. B. ErwGr. 5 der SSM-Verordnung.

Verordnung)[11] wurden der EZB gestützt auf Art. 127 Abs. 6 des Vertrags über die Arbeitsweise der Europäischen Union[12] per 4.11.2014 Kompetenzen zur laufenden und direkten Aufsicht von Instituten in Euroländern übertragen. Die laufende Aufsicht wurde somit auf eine neue und europäisch zentralisierte Ebene gehoben und dadurch eine Säule der Bankenunion verwirklicht, welche bereits im Jahr 2012 auf den Weg gebracht wurde und neben einer einheitlichen europäischen Beaufsichtigung von Banken auch eine einheitliche europäische Abwicklung von ausfallenden Banken zum Ziel hatte.[13] Zudem war auch ein europäisches Einlagensicherungssystem, *European Deposit Insurance Scheme* (EDIS), vorgesehen, zu welchem ein Kommissionsvorschlag vorlag.[14] Im Gegensatz zum SSM und dem einheitlichen Abwicklungsmechanismus, dem *Single Resolution Mechanism* (SRM),[15] welcher seit Jänner 2016 operativ ist, wurde ein europäisches Einlagensicherungssystem bis dato nicht verwirklicht. Parallel zum SSM wurde der ESFS und – als Teil davon – die EBA mit ihren Aufgabenbereichen, die auch jene Länder umschließt, welche den Euro nicht als Währung (Nicht-Euroländer) haben, beibehalten und eine enge Kooperation der Systeme SSM und ESFS festgeschrieben.[16]

### *2. Der einheitliche Aufsichtsmechanismus (SSM) – Struktur und Prinzipien, Hauptkompetenzen*

Der SSM setzt sich aus der EZB mit Sitz in Frankfurt am Main und den nationalen zuständigen Aufsichtsbehörden zusammen. Rechtsgrundlagen bilden die SSM-Verordnung und die SSM-Rahmenverordnung,[17] welche die Zusammenarbeit zwischen der EZB und den nationalen zuständigen Behörden innerhalb des SSM ausgestaltet. Grundsätzlich wurden der EZB Aufsichtstätigkeiten für alle Banken in allen Euro-

---

[11] Verordnung (EU) Nr. 1024/2013 des Rates vom 15. Oktober 2013 zur Übertragung besonderer Aufgaben im Zusammenhang mit der Aufsicht über Kreditinstitute auf die Europäische Zentralbank, ABl. L 287/63 vom 29.10.2013.

[12] Vertrag über die Arbeitsweise der Europäischen Union (konsolidierte Fassung), ABl. C 202/47 vom 7.6.2016.

[13] Siehe hierzu die Mitteilung der Kommission an das Europäische Parlament und den Rat „Fahrplan für eine Bankenunion", Brüssel, den 12.9.2012, COM(2012) 510 final.

[14] Siehe hierzu den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 806/2014 im Hinblick auf die Schaffung eines europäischen Einlagenversicherungssystems, Straßburg, den 24.11.2015, COM(2015) 586 final, 2015/0270 (COD).

[15] Verordnung (EU) Nr. 806/2014 des Europäischen Parlaments und des Rates vom 15. Juli 2014 zur Festlegung einheitlicher Vorschriften und eines einheitlichen Verfahrens für die Abwicklung von Kreditinstituten und bestimmten Wertpapierfirmen im Rahmen eines einheitlichen Abwicklungsmechanismus und eines einheitlichen Abwicklungsfonds sowie zur Änderung der Verordnung (EU) Nr. 1093/2010, ABl. L 225/1 vom 30.7.2014.

[16] Art. 3 SSM-Verordnung, siehe auch ErwGr. 31 und 32 der SSM-Verordnung.

[17] Verordnung (EU) Nr. 468/2014 der Europäischen Zentralbank vom 16. April 2014 zur Einrichtung eines Rahmenwerks für die Zusammenarbeit zwischen der Europäischen Zentralbank und den nationalen zuständigen Behörden und den nationalen benannten Behörden innerhalb des einheitlichen Aufsichtsmechanismus (SSM-Rahmenverordnung) (EZB/2014/17), ABl. L 141/1 vom 14.5.2014.

ländern für jene Aufgaben übertragen, welche in Art. 4 Abs. 1 SSM-Verordnung genannt werden.[18] Allerdings findet eine organisatorische Aufgabenteilung zwischen der EZB und den nationalen Aufsichtsbehörden statt.

Für bedeutende Kreditinstitute (oder Kreditinstitutsgruppen), Finanzholdinggesellschaften und gemischte Finanzholdinggesellschaften, bekannt auch unter dem englischen Begriff *significant institutions* (SIs), welche anhand der Kriterien der Größe, ihrer wirtschaftlichen Bedeutung und grenzüberschreitenden Tätigkeiten ermittelt werden, erfolgt die Aufsicht durch die EZB direkt.[19] Die Einstufung erfolgt kraft Beschlusses der EZB. Jene Kreditinstitute, Finanzholdinggesellschaften oder gemischte Finanzholdinggesellschaften, die die Kriterien für eine Einstufung als bedeutend nicht erfüllen, werden als weniger bedeutend eingestuft, bekannt auch unter dem englischen Begriff *less significant institutions* (LSIs). Die direkte Aufsicht erfolgt für diese durch die national zuständigen Aufsichtsbehörden, *national competent authorities* (NCA), und unter Koordinierung auf EZB-Ebene, soweit es sich nicht um gemeinsame Aufsichtsaufgaben handelt, die unabhängig von der Einstufung der Banken als bedeutend oder weniger bedeutend ausschließlich der EZB übertragen wurden.[20]

Grundsätzlich hat im Rahmen des SSM, und damit auch bei der beschriebenen Aufgabenteilung, die EZB sicherzustellen, dass der SSM wirksam und einheitlich funktioniert.[21] Um eine einheitliche Aufsicht sicherzustellen, wurden eigene Bereiche innerhalb der EZB eingerichtet.[22] Zudem hält die SSM-Verordnung den Grundsatz zu loyaler Zusammenarbeit und Informationsaustausch zwischen EZB und nationalen Aufsichtsbehörden sowie die Unterstützung der EZB durch die nationalen Aufsichtsbehörden fest.[23]

---

[18] Siehe hierzu auch ausführlich EuG, Urt. v. 16.5.2017 – Rs. T-122/15 (Landeskreditbank Baden-Württemberg/EZB), mit welchem das Gericht bestätigte, dass der EZB für sämtliche Kreditinstitute die Zuständigkeit für die Aufsichtsaufgaben, welche in Art. 4 Abs. 1 der SSM-Verordnung gelistet werden, übertragen wurde und nicht nur für bedeutende Kreditinstitute. Siehe insbesondere Rn. 54 ff. Über den Euroländerbereich hinaus besteht auch die Möglichkeit, eine Zusammenarbeit mit den zuständigen Behörden anderer EU-Mitgliedstaaten einzugehen. Siehe hierzu Art. 7 SSM-Verordnung. Derzeit besteht eine solche Zusammenarbeit mit Bulgarien, siehe hierzu Beschluss (EU) 2020/1015 der Europäischen Zentralbank vom 24. Juni 2020 zur Eingehung einer engen Zusammenarbeit zwischen der Europäischen Zentralbank und der Българска народна банка (Bulgarische Nationalbank) (EZB/2020/30), ABl. LI 224/1 vom 13.7.2020.

[19] Siehe Art. 6 SSM-Verordnung und zur Einstufung eines Kreditinstitutes im Detail Art. 39 ff. SSM-Rahmenverordnung.

[20] Siehe Art. 4 Abs. 1 lit. a und c in Verbindung mit Art. 6 Abs. 4 SSM-Verordnung. Es handelt sich um die Zulassung oder den Entzug einer Zulassung von Kreditinstituten und die Durchführung der Beurteilung des Erwerbs oder der Veräußerung qualifizierter Beteiligungen an Kreditinstituten.

[21] Art. 6 Abs. 1 SSM-Verordnung.

[22] Siehe Details im Aufsichtshandbuch. Aufsicht über bedeutende Institute, 2024, 11 f., abrufbar unter https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.supervisory_guides202401_manual.de.pdf (Abrufdatum: 25.7.2024).

[23] Art. 6 Abs. 2 und 3 SSM-Verordnung.

Die EZB kann im Rahmen der ihr kraft Art. 4 Abs. 1 SSM-Verordnung übertragenen Aufgaben Maßnahmen ergreifen und Beschlüsse fassen, wie z. B. über die Eignung der Mitglieder eines Leitungsorganes eines Kreditinstitutes, zu Eigenkapitalanforderungen, zu Liquiditätsanforderungen, zu Großkreditgrenzen und Veröffentlichungen, sie kann Vor-Ort-Prüfungen bei Kreditinstituten vornehmen und Verordnungen erlassen.[24] Ebenso kann sie Beschlüsse zu Durchsetzungsmaßnahmen und Sanktionen gegen *significant institutions* fassen und in speziellen Fällen auch gegen *less signficiant institutions*.[25] Diese auf die mikroprudenzielle Ebene bezogenen Werkzeuge werden durch solche auf der makroprudenziellen ergänzt, indem z. B. höhere Kapitalpuffer als auf nationaler Ebene angeordnet und festgesetzt werden können.[26]

### *3. Der SSM – Governance und Entscheidungsprozesse*

Die EZB führt ihre Aufsichtsaufgaben in strenger Trennung von den Aufgaben der Geldmarktpolitik durch.[27] Um der Trennung der Aufgabenbereiche der EZB bestmöglich Rechnung zu tragen, wurde innerhalb der EZB eine eigene Organisationsstruktur für die Aufsichtsaufgaben geschaffen. Die Planung und Ausführung der Tätigkeiten im *Single Supervisory Mechanism* erfolgt durch ein Aufsichtsgremium, dem *Supervisory Board*, bestehend aus einer/einem Vorsitzenden, der/dem stellvertretenden Vorsitzenden, vier EZB-Repräsentantinnen/Repräsentanten und einer Repräsentantin/einem Repräsentanten aus jeder nationalen zuständigen Aufsichtsbehörde der teilnehmenden Mitgliedstaaten, wobei alle Mitglieder im Interesse der Union zu handeln haben. Das *Supervisory Board* wird durch einen Lenkungsausschuss, dem *Steering Committee*, welcher aus Mitgliedern des *Supervisory Boards* zusammengesetzt ist, und ein Sekretariat bei den Tätigkeiten und Beschlussvorbereitungen unterstützt.

Die laufende Aufsicht über bedeutende Institute wird durch gemeinsame Aufsichtsteams, *Joint Supervisory Teams* (JSTs), welche aus EZB-Mitarbeiterinnen/Mitarbeitern und Aufseherinnen/Aufsehern von nationalen zuständigen Aufsichtsbehörden bestehen, in deren Ländern die *significant institutions*, ihre Tochterunternehmen oder bedeutende ausländische tätige Zweigniederlassungen niedergelassen sind.[28] Diese werden von weiteren Teams, wie z. B. horizontalen Teams mit Spezialwissen zu verschiedenen Bereichen, wie z. B. Kreditrisiken, nichtfinanziellen Risiken, Ge-

[24] Art. 10 ff. SSM-Verordnung, insbesondere Art. 16 SSM-Verordnung.

[25] Art. 18 SSM-Verordnung und Art. 122 SSM-Rahmenverordnung.

[26] Art. 5 SSM-Verordnung zu makroprudenziellen Aufgaben und Instrumenten.

[27] Explizit in Art. 25 SSM-Verordnung und Art. 13k der Geschäftsordnung der Europäischen Zentralbank festgehalten. Zur Geschäftsordnung siehe: Beschluss der Europäischen Zentralbank vom 19. Februar 2004 zur Verabschiedung der Geschäftsordnung der Europäischen Zentralbank (EZB/2004/2) (2004/257/EG), ABl. L 080/33 vom 18.3.2004.

[28] Aufsichtshandbuch. Aufsicht über bedeutende Institute, 2024, 9 ff., abrufbar unter https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.supervisory_guides202401_manual.de.pdf (Abrufdatum: 25.7.2024).

schäftsmodellen, Kapitalplanung, Aufsichtspolitik und Aufsichtsmethoden unterstützt.[29]

Beschlüsse der EZB können jedoch nur durch den EZB-Rat, dem *Governing Council*, welcher sich aus dem EZB-Direktorium und den Gouverneuren/Gouverneurinnen der nationalen Zentralbanken der Euroländer zusammensetzt, gefasst werden. Um dennoch eine bestmögliche Trennung von den Aufsichtsaufgaben zu erreichen, wurde ein eigener Beschlussfassungsprozess aufgesetzt. Das *Supervisory Board* schlägt dem *Governing Council* Beschlussentwürfe zur Annahme vor. Dieser kann innerhalb einer Frist von höchstens zehn Arbeitstagen lediglich widersprechen, die Beschlussentwürfe jedoch nicht inhaltlich abändern.[30] Bei Widerspruch kann das *Supervisory Board* den Beschlussentwurf abändern. Um Meinungsverschiedenheiten beizulegen, wurde auch eine Schlichtungsstelle eingerichtet.[31]

Die EZB ist dem Europäischen Parlament und dem Rat der Europäischen Union rechenschaftspflichtig und legt diesen sowie der Kommission und der Euro-Gruppe jährlich einen Bericht über die Ausübung der Tätigkeiten, welche ihr durch die SSM-Verordnung übertragen wurden, vor.[32] Weiters prüft der Europäische Rechnungshof auch die Tätigkeiten der EZB im übertragenen Bereich der Aufsichtsaufgaben.[33]

Beschlüsse der EZB können einerseits durch den Administrativen Überprüfungsausschuss, das *Administrative Board of Review* (ABoR), einen internen Ausschuss zusammengesetzt aus fünf unabhängigen Experten/Expertinnen, überprüft werden.[34] Dieser gibt nach Prüfung der Zulässigkeit des Überprüfungsantrages eine Stellungnahme gegenüber dem *Supervisory Board* ab, welches dieser Stellungnahme jedoch nicht folgen muss.[35] Unabhängig davon steht der Weg offen, ein Verfahren vor dem EuGH zu führen.[36]

---

[29] Für weitere Details zur Organisationsstruktur siehe Aufsichtshandbuch. Aufsicht über bedeutende Institute, 2024, 8 ff., abrufbar unter https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.supervisory_guides202401_manual.de.pdf (Abrufdatum: 25.7.2024).

[30] Art. 26 Abs. 6 SSM-Verordnung.

[31] Verordnung (EU) Nr. 673/2014 der Europäischen Zentralbank vom 2. Juni 2014 über die Einrichtung einer Schlichtungsstelle und zur Festlegung ihrer Geschäftsordnung (EZB/2014/26), ABl. L 179/72 vom 19.6.2014.

[32] Art. 20 Abs. 1 und 2 SSM-Verordnung.

[33] Art. 20 Abs. 7 SSM-Verordnung.

[34] Art. 24 SSM-Verordnung.

[35] Art. 24 Abs. 7 SSM-Verordnung und des Weiteren Art. 16 und 17 Beschluss der Europäischen Zentralbank vom 14. April 2014 zur Einrichtung eines administrativen Überprüfungsausschusses und zur Festlegung der Vorschriften für seine Arbeitsweise (EZB/2014/16) (2014/360/EU), ABl. L 175/47 vom 14.6.2014. Siehe weitere Details zum Verfahren vor dem ABoR ebendort. Siehe zur Tätigkeit von ABoR auch https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.aborreview202212~ce9fb4e503.en.pdf (Abrufdatum: 25.7.2024).

[36] Art. 24 Abs. 11 SSM-Verordnung. Zum Rechtsschutz siehe auch *Jedlicka*, Verwaltungsgeldbußen im SSM. Steht der gewährte Rechtsschutz für Kreditinstitute im Einklang mit der Rechtsprechung von EGMR und EuGH? ZFR 2016, 481. Anzumerken ist in dem Zusammenhang, dass im Gegensatz zu anderen EZB-Beschlüssen, die nach Art. 263 AEUV geprüft werden, Beschlüsse,

### *4. Der SSM – Materielles Recht*

Die EZB beaufsichtigt die Einhaltung von bankrechtlichen Vorschriften. Als zentrale Rechtsakte sind hier die Richtlinie 2013/36/EU,[37] auch Eigenkapitalrichtlinie oder *Capital Requirements Directive* (CRD), und die Verordnung (EU) Nr. 575/2013,[38] auch Kapitaladäquanzverordnung oder *Capital Requirements Regulation* (CRR), zu nennen, welche ein einheitliches Regelwerk für Kreditinstitute in der EU darstellen und auf europäischer Ebene die vom Basler Ausschuss, *Basel Committee on Banking Supervision* (BCBS),[39] ausgearbeiteten globalen Bankenaufsichts-Standards umsetzen.[40] Diese werden durch zahlreiche andere einschlägige Regelungen ergänzt, wie z. B. den bereits erwähnten technischen Standards (RTS und ITS), welche von der EBA ausgearbeitet und von der Kommission erlassen werden und technische Details regeln, die in der CRR und der CRD nicht abschließend behandelt wurden, oder EZB-Verordnungen und EZB-Beschlüsse.[41] Hauptbestandteile der CRR sind Regeln zu Eigenkapitalqualität und -höhe, Liquidität, Großkrediten, Verschuldungsquote, Meldewesen und Veröffentlichung. Im Hinblick auf Sanktionen ist hervorzuheben, dass die CRD einen Mindestkatalog vorsieht, wonach Verstößen gegen nationale Umsetzungen der CRD oder direkt anwendbare Bestimmungen der CRR auf nationaler Ebene Verwaltungssanktionen oder andere Verwaltungsmaßnahmen nach sich

---

welche gem. Art. 18 Abs. 7 SSM-Verordnung erlassen wurden, Art. 5 Verordnung (EG) 2532/98 folgend nach Art. 261 AEUV geprüft werden.

[37] Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG, ABl. L 176/338 vom 27.6.2013, auch bekannt unter dem Namen vierte Eigenkapitalrichtlinie.

[38] Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 646/2012, ABl. L 176/1 vom 27.6.2013.

[39] Das BCBS setzt globale Standards im Bereich der Bankenregulierung und setzt sich aus Mitgliedern aus Organisationen mit direkter Bankenaufsichtstätigkeit und Zentralbanken zusammen. Da die erarbeiteten Standards keine Rechtskraft haben, hat der BCBS auf das Mitwirken der Mitglieder und die Umsetzung der Standards in den jeweiligen Jurisdiktionen zu setzen. Siehe hierzu auch auf der Homepage der *Bank for International Settlements* (BIS) die Charter des BCBS, abrufbar unter https://www.bis.org/bcbs/charter.htm (Abrufdatum: 25.7.2024).

[40] Siehe z. B. auch ErwGr. 1, 10 und 41 der Richtlinie 2013/36/EU. Im Wesentlichen war die Richtlinie 2013/36/EU bis zum 31.12.2013 umzusetzen, siehe dort Art. 162, und die Verordnung (EU) Nr. 575/2013 war im Wesentlichen ab dem 1.1.2014 anzuwenden, siehe dort Art. 521.

[41] Zum Thema EZB-Beschlüsse und EZB-Verordnungen siehe im Detail *Bax/Witte*, The taxonomy of ECB instruments available for banking supervision, ECB Economic Bulletin 2019, Iss. 6, Kapitel 2.2. und 2.3., abrufbar unter https://www.ecb.europa.eu/press/economic-bulletin/articles/2019/html/ecb.ebart201906_02~3e2f0e4f63.en.html (Abrufdatum: 25.7.2024). Als Beispiel für eine Verordnung siehe Verordnung (EU) 2020/605 der Europäischen Zentralbank vom 9. April 2020 zur Änderung der Verordnung (EU) 2015/534 über die Meldung aufsichtlicher Finanzinformationen (EZB/2020/22), ABl. L 145/1 vom 7.5.2020. In dem Zusammenhang fällt auch häufig der Begriff „*Single Rulebook*". Unter diesem Begriff versteht man ein Paket aus Rechtsakten zur Bankenaufsicht, wobei als Kernbestandteil insbesondere die CRR und CRD zu benennen sind. Siehe auch *Bax/Witte*, ECB Economic Bulletin 2019, Iss. 6, Kapitel 2.2.

ziehen müssen. Diese sollten wirksam, verhältnismäßig und abschreckend sein und in der Regel auch veröffentlicht werden.[42] Die CRD und die CRR wurden in den Jahren 2019[43] und 2024[44] größeren Anpassungen unterzogen, wobei insbesondere die Änderungen im Jahr 2024[45] weitergehende Regeln auch im Bereich von Durchsetzungsmaßnahmen und Sanktionen vorsehen. So wurde der erwähnte Mindestkatalog erweitert und zudem periodisch zu verhängende Zwangsgelder als im nationalen Recht vorzusehendes Instrument eingeführt. Diese Zwangsgelder sind periodisch pekuniäre Durchsetzungsmaßnahmen, die auf die Beendigung von anhaltenden Verstößen gegen nationale Bestimmungen zur Umsetzung der CRD, CRR oder Verstößen gegen Rechtsakte, die auf Grundlage der CRD und CRR von zuständigen Behörden erlassen wurden, abzielen. Sie sollen natürliche oder juristische Personen dazu veranlassen, den aufrechten Verstoß zu beenden.[46] Zudem wurde verankert, dass eine Verhängung dieser Zwangsgelder die zuständigen Behörden nicht daran hindern soll, für denselben Verstoß Verwaltungssanktionen oder andere Verwaltungsmaßnahmen zu verhängen.[47]

---

[42] Siehe hierzu Art. 67 Abs. 1 Richtlinie 2013/36/EU und ErwGr. 35 und 36, sowie zu den Veröffentlichungen insbesondere Art. 68 Richtlinie 2013/36/EU und zur abschreckenden Wirkung durch die Veröffentlichung ErwGr. 38.

[43] Richtlinie (EU) 2019/878 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Änderung der Richtlinie 2013/36/EU im Hinblick auf von der Anwendung ausgenommene Unternehmen, Finanzholdinggesellschaften, gemischte Finanzholdinggesellschaften, Vergütung, Aufsichtsmaßnahmen und -befugnisse und Kapitalerhaltungsmaßnahmen, ABl. L 150/253 vom 17.6. 2019; Verordnung (EU) 2019/876 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Änderung der Verordnung (EU) Nr. 575/2013 in Bezug auf die Verschuldungsquote, die strukturelle Liquiditätsquote, Anforderungen an Eigenmittel und berücksichtigungsfähige Verbindlichkeiten, das Gegenparteiausfallrisiko, das Marktrisiko, Risikopositionen gegenüber zentralen Gegenparteien, Risikopositionen gegenüber Organismen für gemeinsame Anlagen, Großkredite, Melde- und Offenlegungspflichten und der Verordnung (EU) Nr. 648/2012, ABl. L 150/1 vom 7.6.2019.

[44] Richtlinie (EU) 2024/1619 des Europäischen Parlaments und des Rates vom 31. Mai 2024 zur Änderung der Richtlinie 2013/36/EU im Hinblick auf Aufsichtsbefugnisse, Sanktionen, Zweigstellen aus Drittländern sowie Umwelt-, Sozial- und Unternehmensführungsrisiken, ABl. L 68/2 vom 19.6.2024, auch bezeichnet als CRD VI; Verordnung (EU) 2024/1623 des Europäischen Parlaments und des Rates vom 31. Mai 2024 zur Änderung der Verordnung (EU) Nr. 575/2013 im Hinblick auf Vorschriften für das Kreditrisiko, das Risiko einer Anpassung der Kreditbewertung, das operationelle Risiko, das Marktrisiko und die Eigenmitteluntergrenze (Output-Floor), ABl. L 189/1 vom 19.6.2024, auch bezeichnet als CRR III.

[45] Die Änderungen der CRD sind im Wesentlichen bis 10.1.2026 umzusetzen, siehe hierzu Art. 2 der Richtlinie (EU) 2024/1619. Die Bestimmungen der CRR sind ab 1.1.2025 anzuwenden.

[46] Zum Begriff der Zwangsgelder siehe künftig Art. 3 Abs. 1 Z. 67 der CRD und zur Ausgestaltung die künftige Fassung des Art. 66 Abs. 2 lit. b CRD.

[47] Siehe Art. 1 Abs. 16 Richtlinie (EU) 2024/1619 zur künftigen Fassung des Art. 65 Abs. 3 CRD.

## III. Der einheitliche Bankenaufsichtsmechanismus – Verwaltungssanktionen und Durchsetzungsmaßnahmen

### *1. Einführende Bemerkungen*

Die EZB ist im Rahmen des SSM mit Sanktionskompetenzen in Form von Geldbußen und mit Durchsetzungsmaßnahmen wie Zwangsgeldern ausgestattet worden. Die Ausstattung mit Sanktionskompetenzen ist einerseits die Weiterführung des Gedankens, wie insbesondere im *de Larosière*-Report analysiert, aber auch vom BCBS nach der Finanzkrise in den *Core Principles for Effective Banking Supervision* hervorgehoben, dass es für eine wirkungsvolle Aufsicht zur Gewährleistung der Einhaltung der Aufsichtsregeln neben anderen Maßnahmen auch Sanktionen benötigt, die wirksam, verhältnismäßig und abschreckend sein sollen. Andererseits wird durch die Ausstattung der EZB mit den genannten Kompetenzen eine einheitliche Anwendung in den Euroländern ermöglicht.[48] Die Kernbestimmungen zu den Verwaltungssanktionen und Durchsetzungsmaßnahmen auf materieller und prozessualer Ebene, welche in der SSM-Verordnung, der SSM-Rahmenverordnung sowie in der Verordnung (EG) Nr. 2532/98 des Rates vom 23.11.1998[49] zu finden sind, werden in der Folge anhand von ausgewählten Fallkonstellationen dargestellt. An dieser Stelle sei auch auf andere Maßnahmen, die der EZB gem. Art. 16 SSM-Verordnung zur Verfügung stehen, wie z. B. höhere Eigenmittel zur Bedeckung von Risiken zu verlangen, Geschäftstätigkeiten einzuschränken oder Dividendenauszahlungseinschränkungen oder -verbote zu verhängen, sowie auf die ausschließliche Kompetenz der EZB gem. Art. 14 Abs. 5 SSM-Verordnung Banklizenzen zu entziehen, verwiesen, welche hier aber nicht behandelt werden.

### *2. Verteilung der Kompetenzen zwischen EZB und national zuständigen Aufsichtsbehörden*

Wie sogleich im Rahmen von Fallkonstellationen erörtert wird, stehen der EZB nur in bestimmten Fällen Sanktionskompetenzen und Durchsetzungsmaßnahmen zur Verfügung. Abhängig davon, gegen welche Norm verstoßen wurde, ob gegen eine juristische oder eine natürliche Person vorgegangen werden soll, ob es sich um ein bedeutendes oder ein weniger bedeutendes Institut handelt und ob eine Verwaltungs-

---

[48] Report of the High-Level Group on Financial Supervision in the EU, 2009, abrufbar unter https://ec.europa.eu/economy_finance/publications/pages/publication14527_en.pdf, (Abrufdatum: 25.7.2024). Siehe insbesondere Rn. 83 ff., 160, 198 ff. BCBS Core Principles for Effective Banking Supervision vom 14.9.2012, Principle 11, abrufbar unter https://www.bis.org/publ/bcbs230.pdf (Abrufdatum: 25.7.2024). Diese wurden in Folge überarbeitet und im April 2024 veröffentlicht, abrufbar unter: https://www.bis.org/bcbs/publ/d573.pdf (Abrufdatum: 25.7.2024), nunmehr auch im konsolidierten Basel Framework enthalten, abrufbar unter https://www.bis.org/baselframework/Basel Framework.pdf (Abrufdatum: 25.7.2024).

[49] Verordnung (EG) Nr. 2532/98 des Rates vom 23. November 1998 über das Recht der Europäischen Zentralbank, Sanktionen zu verhängen, ABl. L 318/4 vom 27.11.1998.

geldbuße oder eine andere Maßnahme oder eine nicht in Geld bemessene Sanktion verhängt werden soll, verteilen sich die Kompetenzen zwischen der EZB und den national zuständigen Aufsichtsbehörden.

### *3. Fallstudie 1 – CRR-Verstoß und direkte Sanktionsmöglichkeit der EZB*

Die EZB stellt fest, dass ein bedeutendes, direkt von ihr beaufsichtigtes Kreditinstitut (*significant institution*) gegen Bestimmungen betreffend Großkredite gem. Art. 395 CRR verstieß, indem es die in der CRR festgelegten Obergrenzen für Großkredite für einen Zeitraum von mehreren Monaten überschritt. Das Kreditinstitut hatte nicht sichergestellt, dass bei der Kreditvergabe ausreichende Prüfungen der anwendbaren Obergrenzen stattfinden.

Die Kernbestimmungen in der SSM-Verordnung im Hinblick auf Sanktionsmöglichkeiten sind in Art. 18 SSM-Verordnung enthalten. Art. 18 Abs. 1 SSM-Verordnung legt fest, dass die EZB über direkt von ihr beaufsichtigte Kreditinstitute, Finanzholdinggesellschaften oder gemischte Finanzholdinggesellschaften Verwaltungsgeldbußen verhängen kann, wenn diese vorsätzlich oder fahrlässig gegen eine Anforderung aus direkt anwendbaren Rechtsakten verstoßen, so den zuständigen Behörden nach dem Unionsrecht wegen dieses Verstoßes die Möglichkeit zur Verfügung gestellt wird, Verwaltungsgeldbußen zu verhängen.

Im konkreten Sachverhalt handelt es sich um einen Verstoß gegen Art. 395 CRR, eine EU-Verordnung, sohin einen direkt anwendbaren Rechtsakt der Union. Die weitere Voraussetzung nach Art. 18 Abs. 1 SSM-Verordnung, die in der deutschen Fassung darauf abstellt, dass „den zuständigen Behörden nach dem Unionsrecht wegen dieses Verstoßes die Möglichkeit, Verwaltungsgeldbußen zu verhängen, zur Verfügung gestellt wird“ ist ebenfalls erfüllt.[50] Für den Verstoß gegen Art. 395 der CRR sind gem. Art. 67 Abs. 1 lit. w der Richtlinie 2013/36/EU Verwaltungssanktionen oder andere Verwaltungsmaßnahmen auf nationaler Ebene jedenfalls vorzusehen.[51]

Im Hinblick auf den Sachverhalt sind die Voraussetzungen nach Art. 18 Abs. 1 SSM-Verordnung erfüllt und für die EZB besteht die Möglichkeit, für den erfolgten Verstoß gegen Art. 395 CRR durch eine *significant institution* eine Verwaltungsgeldbuße zu verhängen, so darüber hinaus auch das Erfordernis des fahrlässigen oder vorsätzlichen Verhaltens vorliegt. Anzumerken ist, dass Art. 18 Abs. 1 SSM-Verord-

---

[50] Es ist darauf hinzuweisen, dass die authentischen Sprachversionen potentiell verschiedene Auslegungen einer an sich ident (gemeinten) Norm zulassen könnten. So verlangt die englische Fassung z. B. „in relation to which administrative pecuniary penalties shall be made available to competent authorities under the relevant Union law.“ Eine genauere Betrachtung dieses Themas muss an dieser Stelle unterbleiben. Vielmehr ist dem Thema der Ringvorlesung entsprechend darauf hinzuweisen, dass durch die Schaffung des SSM eine einheitlichere Auslegung trotz potentieller Ansatzpunkte für abweichende Auslegungen bedingt durch unterschiedliche Sprachumsetzung gefördert und somit Rechtssicherheit für Normunterworfene geschaffen wird, zweifelsohne ein gemeinsames Interesse, dem der SSM hier Rechnung trägt.

[51] Lit. k bis zur Änderung ab 9.7.2024 durch die Richtlinie (EU) 2024/1619.

nung der EZB zwar das Recht einräumt, eine Verwaltungsgeldbuße zu verhängen; verpflichtet wird sie dem Wortlaut folgend („kann […] verhängen") jedoch nicht dazu. Somit hat die EZB auch die Möglichkeit, einen einheitlichen Ansatz und eine einheitliche Strategie im Euroraum zu entwickeln, für welche Verstöße eine Verwaltungsgeldbuße verhängt werden soll, und ebenso die Entscheidungshoheit, welche Höhe eine solche haben soll.[52]

Für Verfahren nach Art. 18 Abs. 1 SSM-Verordnung ist prozessual auf die Bestimmungen der Art. 120 ff. der SSM-Rahmenverordnung abzustellen. Diese bestimmen im Ermittlungsverfahren die Einrichtung einer unabhängigen Untersuchungsstelle und deren Befugnisse, die Verfahrensrechte, die Prüfung der Akte der Untersuchungsstelle durch das *Supervisory Board* sowie Verjährungsfristen für die Verhängung und Durchsetzung von Verwaltungssanktionen.

### *4. Exkurs zur Berechnung der Verwaltungsgeldbuße*

Eine Geldbuße nach Art. 18 Abs. 1 der SSM-Verordnung kann bis zu 10 % des jährlichen Gesamtumsatzes (im Sinne des einschlägigen Unionsrechts) einer juristischen Person im vorangegangenen Geschäftsjahr oder bis zur zweifachen Höhe der aufgrund des Verstoßes erzielten Gewinne oder verhinderten Verluste, so diese beziffert werden können, betragen. Zur Berechnung der Höhe einer Verwaltungsgeldbuße hat die EZB im März 2021 den sogenannten „*Guide to the method of setting administrative pecuniary penalties*" veröffentlicht.[53] Dieser Guide beschreibt, welche Kriterien die EZB zur Festsetzung von Verwaltungsgeldbußen heranzieht. Es wird zunächst ein Grundbetrag ermittelt, welcher in Folge weiter angepasst wird.[54] Zur Ermittlung des Grundbetrages dienen (um eine Verhältnismäßigkeit zu garantieren) die Größe des Institutes sowie die Schwere des Verstoßes als Bemessungskriterien. Die Schwere des Verstoßes wird in fünf Kategorien von gering bis äußerst schwer untergliedert. Für die Einordnung maßgeblich sind die Auswirkungen des Verstoßes einerseits und das Ausmaß des Fehlverhaltens andererseits.[55] Die Auswirkungen des Verstoßes werden ebenso untergliedert. Unterschieden wird zwischen niedrigen, mittleren und

---

[52] Als Beispiel für eine Verwaltungsgeldbuße der EZB betreffend Art. 395 CRR siehe den finalen EZB-Beschluss vom 13.8.2019 gem. Art. 18 Abs. 1 SSM-Verordnung betreffend den Verstoß gegen Obergrenzen für Großkredite gem. Art. 395, abrufbar unter https://www.bankingsupervision.europa.eu/banking/sanctions/html/index.en.html (Abrufdatum: 25.7.2024).

[53] Guide to the method of setting administrative pecuniary penalties pursuant to Article 18(1) and (7) of Council Regulation (EU) No 1024/2013, abrufbar unter https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.guidetothemethodofsettingadministrativepecuniarypenalties_202103~400cbafa55.de.pdf (Abrufdatum: 25.7.2024).

[54] Guide to the method of setting administrative pecuniary penalties pursuant to Article 18(1) and (7) of Council Regulation (EU) No 1024/2013, 3. Auf eine zweistufige Methode wurde seitens der EZB in einem früheren Gerichtsverfahren hingewiesen, siehe EuG, Urt. v. 8.7.2020 – Rs. T-576/18 (Crédit agricole/EZB) – Rn. 125. In diesem befasste sich das Gericht auch mit der Begründungspflicht zur Höhe der verhängten Verwaltungsgeldbuße.

[55] Guide to the method of setting administrative pecuniary penalties pursuant to Article 18(1) and (7) of Council Regulation (EU) No 1024/2013, 3.

hohen Auswirkungen, und berücksichtigt werden hier unter anderem, welche Auswirkungen der Verstoß auf das Kreditinstitut hatte, wie z. B. die Höhe der Abweichung von rechtlichen Vorschriften – im gegebenen Sachverhalt von Fallstudie 1 könnte dies wohl das Ausmaß der Abweichung von den gesetzlich festgelegten Obergrenzen für Großkredite sein –, welche Auswirkung der Verstoß auf die wirksame Beaufsichtigung des Kreditinstitutes hatte, die Dauer des Verstoßes, der bei Dritten entstandene Schaden oder auch mögliche Auswirkungen auf den Bankensektor insgesamt.[56] Die EZB weist darauf hin, dass bei solchen Vorschriften, welche für die Sicherheit und Solidität des Kreditinstitutes besonders wichtig sind, eine geringere Abweichung von der rechtlichen Vorgabe bereits zu einer höheren Einstufung in der Auswirkung des Verstoßes führen kann.[57] Beim Ausmaß des Fehlverhaltens unterscheidet die EZB zwischen drei Kategorien (niedrig, mittel und hoch), wobei für die Einstufung der Grad des fahrlässigen oder vorsätzlichen Handelns Kriterium ist.[58]

Während für äußerst schwere Verstöße die Verwaltungsgeldbuße auf Basis eines Prozentsatzes des jährlichen Gesamtumsatzes des Kreditinstitutes berechnet wird, dient für die Bemessung sonst, so keine Ermittlung anhand der durch den Verstoß erzielten Gewinne oder verhinderten Verluste stattfindet, ein Raster, in welchem abgestuft nach der Schwere des Verstoßes, der wie zuvor beschrieben ermittelt wird, verschiedene Grundbeträge vorgesehen sind, wobei diese an die Größe des Kreditinstitutes, bemessen an seinen Vermögenswerten, gekoppelt sind.[59] Im Raster sind die Kreditinstitute verschiedenen Größengruppen zugeordnet, es erfolgt jedoch kreditinstitutsindividuell nach Vermögenswerten und auf Basis von erschwerenden oder mildernden Umständen eine Anpassung des Grundbetrages. Die EZB erwähnt hier ausdrücklich, dass die Gegebenheiten des Einzelfalles ein Abweichen von der im Guide beschriebenen Berechnungsmethode notwendig machen können, und erwähnt im Einklang mit dem Grundsatz, welcher auch in Art. 18 Abs. 1 SSM-Verordnung festgehalten ist, dass die Verwaltungsgeldbuße wirksam, verhältnismäßig und abschreckend sein muss.[60]

Auch anhand dieses Guides, welcher transparent die Berechnungsmethoden der EZB darstellt, kann hervorgehoben werden, dass durch die Schaffung des SSM dem gemeinsamen Interesse der Rechtssicherheit Rechnung getragen wird, da neben einer einheitlichen Anwendung der aufsichtsrechtlichen Bestimmungen, insbesondere

---

[56] Guide to the method of setting administrative pecuniary penalties pursuant to Article 18(1) and (7) of Council Regulation (EU) No 1024/2013, 3.

[57] Guide to the method of setting administrative pecuniary penalties pursuant to Article 18(1) and (7) of Council Regulation (EU) No 1024/2013, 3.

[58] Guide to the method of setting administrative pecuniary penalties pursuant to Article 18(1) and (7) of Council Regulation (EU) No 1024/2013, 4.

[59] Guide to the method of setting administrative pecuniary penalties pursuant to Article 18(1) and (7) of Council Regulation (EU) No 1024/2013, 4 ff.

[60] Guide to the method of setting administrative pecuniary penalties pursuant to Article 18(1) and (7) of Council Regulation (EU) No 1024/2013, 1 ff. Zudem wird darauf hingewiesen, dass der Guide keine Basis für eine automatisierte Berechnung darstellt.

auch im Hinblick auf die Feststellung von Verstößen, auch eine einheitliche Herangehensweise bei der Bemessung von Verwaltungsgeldbußen stattfindet.

### *5. Fallstudie 2 – Verstoß gegen einen EZB-Beschluss und direkte Sanktionsmöglichkeit der EZB*

Bei demselben wie unter Fallstudie 1 genannten Kreditinstitut wird ein Verstoß gegen bestimmte Meldeanforderungen, welche die EZB im Rahmen der Aufsichtsaufgaben, welche ihr mit der SSM-Verordnung übertragen wurden, gegenüber dem Institut rechtskräftig erlassen hatte, festgestellt.

Im Fall eines Verstoßes gegen einen EZB-Beschluss kann die EZB kraft Art. 18 Abs. 7 SSM-Verordnung in Verbindung mit der Verordnung (EG) Nr. 2532/98[61] eine Verwaltungsgeldbuße verhängen. Wie bei Art. 18 Abs. 1 SSM-Verordnung ist unter Art. 4a Abs. 1 lit. a der Verordnung (EG) Nr. 2532/98 die maximale Höhe für Geldbußen auf 10 % des jährlichen Gesamtumsatzes des Kreditinstitutes[62] oder das Zweifache des aufgrund der Übertretung erzielten Gewinns oder des aufgrund der Übertretung verhinderten Verlustes, sofern sich diese Beträge beziffern lassen, beschränkt. Der Verstoß gegen den EZB-Beschluss ist ausreichend, um eine Verwaltungsgeldbuße verhängen zu können. Ein Blick in andere Rechtsakte, die für eine Sanktionsmöglichkeit wie in Art. 18 Abs. 1 SSM-Verordnung Voraussetzung sind, ist nicht notwendig. Wie schon für Art. 18 Abs. 1 SSM-Verordnung beschrieben, ist die EZB auch gem. Art. 18 Abs. 7 SSM-Verordnung nicht verpflichtet, eine Sanktion zu verhängen. Sollte sich die EZB entschließen, eine solche zu verhängen, bringt die EZB zur Bemessung der Höhe wiederum die im veröffentlichten *Guide to the method of setting administrative pecuniary penalties* dargestellten Kriterien zur Anwendung. Ergänzend ist zu erwähnen, dass der EZB im Rahmen des Art. 18 Abs. 7 SSM-Verordnung in Verbindung mit Art. 122 SSM-Rahmenverordnung auch die Möglichkeit eingeräumt wurde, eine Verwaltungsgeldbuße gegenüber weniger bedeutenden beaufsichtigten Kreditinstituten zu verhängen: und zwar in dem Fall, in dem ein solches Kreditinstitut gegen einen EZB-Beschluss oder eine EZB-Verordnung verstößt, die ihm Verpflichtungen gegenüber der EZB auferlegen.

Für Verfahren zu Verwaltungsgeldbußen nach Art. 18 Abs. 7 SSM-Verordnung ist gem. Art. 121 Abs. 2 SSM-Verordnung auch auf die Verordnung (EG) Nr. 2532/98[63] zu verweisen, insbesondere die Art. 4a, 4b und 4c, wobei die prozessualen Aspekte mit jenen für Verfahren nach Art. 18 Abs. 1 SSM-Verordnung übereinstimmen.

---

[61] Verordnung (EG) Nr. 2532/98 des Rates vom 23. November 1998 über das Recht der Europäischen Zentralbank, Sanktionen zu verhängen, ABl. L 318/4 vom 27.11.1998.

[62] Im Rechtsakt als „Unternehmen" geführt.

[63] Verordnung (EG) Nr. 2532/98 des Rates vom 23. November 1998 über das Recht der Europäischen Zentralbank, Sanktionen zu verhängen, ABl. L 318/4 vom 27.11.1998.

### *6. Fallstudie 3 – Verstoß gegen nationales Recht in Umsetzung der CRD und fehlende direkte Sanktionsmöglichkeit durch die EZB*

Bei demselben wie unter Fallstudie 1 beschriebenen Kreditinstitut wird festgestellt, dass es mit der Vergütungspolitik gegen nationale Bestimmungen, welche eine Umsetzung des Art. 74 CRD darstellen, und auch gegen in diesem Zusammenhang erlassene EBA-Leitlinien, verstößt.

In diesem Fall eines Verstoßes gegen nationales Recht in Umsetzung der CRD scheidet eine Anwendung des Art. 18 Abs. 1 SSM-Verordnung aus, welcher auf den Verstoß gegen einen direkt anwendbaren Rechtsakt der Union abstellt. Ebenso scheidet Art. 18 Abs. 7 SSM-Verordnung aus, da es sich um keinen Verstoß gegen einen EZB-Beschluss oder eine EZB-Verordnung handelt. Für Verstöße gegen nationale Bestimmungen, mit denen einschlägige Richtlinien umgesetzt werden, ist Art. 18 Abs. 5 SSM-Verordnung einschlägig. Über diesen kann die EZB, wenn dies für die Zwecke der Wahrnehmung der ihr durch die SSM-Verordnung übertragenen Aufgaben erforderlich ist, von den nationalen zuständigen Behörden verlangen, Verfahren einzuleiten. Dies mit dem Ziel, dass Maßnahmen ergriffen werden, um sicherzustellen, dass geeignete Sanktionen verhängt werden.[64] Laut Sachverhalt handelt es sich um einen Verstoß gegen Art. 74 CRD durch den Mindestkatalog unter Art. 67 lit. d und t CRD erfasst, und somit ist auf nationaler Ebene eine Sanktionsmöglichkeit vorzusehen.[65] Während die EZB zwar ein Verlangen zur Einleitung eines Verfahrens nach Art. 18 Abs. 5 SSM-Verordnung an die nationale zuständige Aufsichtsbehörde senden kann, obliegt das jeweilige Verfahren dem nationalen Recht und die nationalen Behörden entscheiden, ob, welche und in welcher Höhe eine Sanktion verhängt wird, wobei der Grundsatz, dass die Sanktionen wirksam, verhältnismäßig und abschreckend sein müssen, auch für nationale Behörden in Art. 18 Abs. 5 SSM-Verordnung nochmals explizit festgehalten wird.

Somit ist festzuhalten: *Significant institutions* werden zwar direkt von der EZB beaufsichtigt, die EZB verfügt allerdings über keine direkte Sanktionskompetenz bei einem Verstoß gegen nationales Recht, wenn es sich um eine Umsetzung einer einschlägigen Rechtsnorm aus dem Unionsrecht handelt, wie im Falle des Art. 74 CRD im angegebenen Sachverhalt.

Über den gegebenen Sachverhalt hinaus ist zu ergänzen, dass Art. 18 Abs. 5 SSM-Verordnung auch für andere Fälle angewendet werden kann, nach denen für die EZB keine Sanktionsmöglichkeit nach Art. 18 Abs. 1 SSM-Verordnung besteht, z. B. in Fällen, in denen es sich um einen Verstoß gegen die CRR handelt und eine Sanktion gegen eine natürliche Person verhängt werden soll, oder eine andere Sanktion als eine Verwaltungsgeldbuße.

---

[64] Darüber hinaus kann Art. 18 Abs. 5 SSM-Verordnung, wie im Wortlaut angelegt, auch dann zur Anwendung gebracht werden, wenn ein Verstoß gegen direkt anwendbares Unionsrecht vorliegt und kein europäischer Rechtsakt eine Verpflichtung für eine Sanktionsmöglichkeit vorsieht, aber im nationalen Recht eine Sanktionsmöglichkeit besteht.

[65] Lit. d bis zur Änderung ab 9.7.2024 durch die Richtlinie (EU) 2024/1619.

### *7. Fallstudie 4 – Aufrechter Verstoß gegen einen EZB-Beschluss und direkte Durchsetzungsmaßnahmen der EZB*

Die EZB stellt fest, dass ein bedeutendes, von ihr direkt beaufsichtigtes Kreditinstitut gegen einen rechtskräftigen EZB-Beschluss verstößt und der Verstoß andauert.

Nicht unerwähnt soll an dieser Stelle bleiben, dass gem. Art. 18 Abs. 7 SSM-Verordnung in Verbindung mit Art. 129 SSM-Rahmenverordnung und Art. 1 Abs. 6 Verordnung (EG) Nr. 2532/98 die EZB im Falle eines andauernden Verstoßes gegen einen EZB-Beschluss oder eine EZB-Verordnung in regelmäßigen Abständen zu zahlende Strafgelder, bekannter unter dem englischen Begriff *periodic penalty payments*, auferlegen kann, um einen Zwang zu schaffen, den EZB-Beschluss oder die EZB-Verordnung einzuhalten. Dieses Instrument wurde zuletzt mehrmals von der Presse, aber auch von der EZB in Veröffentlichungen erwähnt.[66] Die *periodic penalty payments* müssen wirksam und verhältnismäßig sein und können gem. Art. 129 Abs. 2 bis 4 SSM-Rahmenverordnung und Art. 4a Verordnung (EG) Nr. 2532/98 bis zu einer Höhe von 5 % des durchschnittlichen Tagesumsatzes pro Tag der Übertretung für einen Zeitraum von maximal sechs Monaten verhängt werden, beginnend ab dem Tag, der in dem Beschluss bezeichnet ist, ab dem die *periodic penalty payments* verhängt werden.

Zwar trägt diese Maßnahme den Begriff „Strafgeld" in sich, dieses Instrument wird jedoch nicht als Strafe angesehen.[67] Tatsächlich ist auch – anders als für Verwaltungsgeldbußen – gem. Art. 129 Abs. 1 letzter Satz SSM-Rahmenverordnung für *periodic penalty payments* das Verfahren gem. Art. 22 der SSM-Verordnung und des Teils III Titel 2, somit Art. 25 ff. der SSM-Rahmenverordnung, anzuwenden, daher jenes für allgemeine Aufsichtsbeschlüsse der EZB. Damit ist, anders als beim Verfahren für Verwaltungsgeldbußen, keine unabhängige Untersuchungsstelle einzu-

---

[66] Artikel in Financial Times, ECB warns of tougher fines for banks that 'drag their feet' on fixing flaws, vom 7.12.2013, abrufbar unter https://www.ft.com/content/028aa0ec-5603-4ca1-b0cc-d9f0849a7a94 (Abrufdatum: 25.7.2024); Artikel in Reuters, Some euro zone banks may be fined after missing ECB climate goal, vom 5.6.2024, abrufbar unter https://www.reuters.com/sustainability/sustainable-finance-reporting/some-euro-zone-banks-may-be-fined-after-missing-ecb-climate-goal-2024-06-05 (Abrufdatum: 25.7.2024); Powers, ability and willingness to act – the mainstay of effective banking supervision, Speech by Frank Elderson, Member of the Executive Board of the ECB and Vice-Chair of the Supervisory Board of the ECB, vom 7.12.2023, abrufbar unter https://www.ecb.europa.eu/press/key/date/2023/html/ecb.sp231207~0a940e45d8.en.html (Abrufdatum: 25.7.2024); Preparing for the next decade of European banking supervision: risk-focused, impactful and legally sound, Speech by Frank Elderson, Member of the Executive Board of the ECB and Vice-Chair of the Supervisory Board of the ECB, vom 27.6.2024, abrufbar unter https://www.bankingsupervision.europa.eu/press/speeches/date/2024/html/ssm.sp240627~6f39f4ba7f.en.html (Abrufdatum: 25.7.2024). Siehe ebenso Aufsichtshandbuch. Aufsicht über bedeutende Institute, 2024, 117 f., abrufbar unter https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.supervisory_guides202401_manual.de.pdf (Abrufdatum: 25.7.2024).

[67] Aufsichtshandbuch. Aufsicht über bedeutende Institute, 2024, 117, abrufbar unter https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.supervisory_guides202401_manual.de.pdf (Abrufdatum: 25.7.2024).

richten, welche vor einem Beschlussvorschlag an das Aufsichtsgremium dem Kreditinstitut Untersuchungsergebnisse und Beschwerdepunkte mitteilt und diesem das Recht einräumt, sich zu den Tatsachen und gegen das Kreditinstitut erhobenen Beschwerdepunkten, einschließlich zu den Bestimmungen, gegen die mutmaßlich verstoßen wurde, zu äußern. Das rechtliche Gehör wird bei *periodic penalty payments* stattdessen durch das *Supervisory Board* eingeräumt.[68] Seit dem Inkrafttreten der Richtline (EU) 2023/2864[69] am 9.7.2024, welche die CRD ändert, erfährt die Beurteilung, dass *periodic penalty payments* keine Sanktionen sind, Verstärkung. Die geänderte Fassung der CRD sieht den Strafgeldern nach SSM-Rahmenverordnung und Verordnung (EG) 2532/98 beinahe idente Durchsetzungsmaßnahmen unter dem Titel Zwangsgelder vor, die zum Ziel haben, natürliche oder juristische Personen zur Beendigung eines andauernden Verstoßes zu bringen und die Behörden nicht daran hindern sollen, wegen desselben Verstoßes Verwaltungssanktionen zu verhängen.[70] Unter dieser Vorgabe sind Zwangsgelder im Sinne der CRD potentiell nicht als Sanktionen zu beurteilen, andernfalls die Vorgabe nach Art. 65 Abs. 3, für denselben Verstoß Verwaltungssanktionen verhängen zu können, Fragestellungen in Bezug auf das Verbot der Doppelbestrafung gem. Art. 50 der Charta der Grundrechte der Europäischen Union und des Art. 4 des 7. Zusatzprotokolls der Europäischen Menschenrechtskonvention aufwerfen würde. Eine genauere Betrachtung muss an dieser Stelle unterbleiben und allfällige einschlägige Gerichtsentscheidungen bei einer Verhängung von *periodic penalty payments* und Sanktionen für denselben Verstoß bleiben abzuwarten.[71]

Jedenfalls wird durch die Änderung der CRD das Portfolio der Aufsichtsbehörden um ein weiteres Werkzeug ergänzt, so diese nicht bereits über ein solches oder ähnliches unter ihrem nationalen Recht verfügten. Allerdings wird auch jenes der EZB ergänzt, da über die Anwendung des Art. 9 Abs. 1 UAbs. 2 der SSM-Verordnung die EZB sämtliche Befugnisse und Pflichten hat, die zuständige und benannte Behörden nach dem einschlägigen Unionsrecht haben, sofern die SSM-Verordnung nichts anderes vorsieht.[72]

---

[68] Siehe zu diesem Verfahren Aufsichtshandbuch. Aufsicht über bedeutende Institute, 2024, 22, abrufbar unter https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.supervisory_guides 202401_manual.de.pdf (Abrufdatum: 25.7.2024).

[69] Richtlinie (EU) 2024/1619.

[70] Siehe Richtlinie (EU) 2024/1619 ErwGr. 30, zur Definition Art. 1 Abs. 2 lit. h Z. 67 (künftig Art. 3 Abs. 1 Z. 67 CRD) sowie Abs. 16 zu Art. 65 Abs. 3 und zu Art. 66 Abs. 2 lit. b.

[71] Siehe vertiefend zum *ne bis in idem* Thema eine Übersicht zu Gerichtsentscheidungen, abrufbar unter https://www.eurojust.europa.eu/publication/case-law-court-justice-european-union-principle-ne-bis-idem-criminal-matters-december-2021 (Abrufdatum: 25.7.2024). Siehe auch EuG, Urt. v. 28.2.2024 – Rs. T-647/21 und T-99/22 (MeSoFa/EZB) zu Abschöpfungszinsen nach § 97 BWG und Verwaltungsgeldbußen. Laut dem Urteil verstößt eine Erhebung von Abschöpfungszinsen für ein Verhalten das bereits Gegenstand einer Verwaltungsgeldbuße der EZB war nicht gegen den Grundsatz *ne bis in idem*.

[72] Siehe im Zusammenhang mit Art. 9 SSM-Verordnung EuGH, Urt. v. 7.8.2018 – Rs. C-52/17 (VTB Bank) betreffend Abschöpfungszinsen nach österreichischem § 97 BWG, für welche der

### *8. Zusammenfassung zu Verwaltungssanktionen und Durchsetzungsmaßnahmen der EZB*

Wie anhand der Fallstudien beleuchtet, werden der EZB im Rahmen des Art. 18 Abs. 1 und Abs. 7 SSM-Verordnung Möglichkeiten eingeräumt, Verwaltungssanktionen zu verhängen. Diese sind jedoch beschränkt auf Verwaltungsgeldbußen über juristische Personen, *in concreto* Kreditinstitute oder (gemischte) Finanzholdinggesellschaften, die direkt von der EZB beaufsichtigt werden.[73] Zudem muss es sich im Fall von Art. 18 Abs. 1 SSM-Verordnung um einen Verstoß gegen einen direkt anwendbaren Rechtsakt der EU handeln, im Fall von Art. 18 Abs. 7 um einen Verstoß gegen einen EZB-Beschluss oder eine EZB-Verordnung. Zudem ist Voraussetzung, so es sich nicht um einen Verstoß gegen einen EZB-Beschluss oder eine EZB-Verordnung handelt, dass den zuständigen Behörden nach dem Unionsrecht wegen dieses Verstoßes die Möglichkeit zur Verfügung gestellt wird, Verwaltungsgeldbußen zu verhängen. Die EZB kann eine Sanktion verhängen, ist hierzu aber nicht verpflichtet.

Wenn die genannten Voraussetzungen nicht gegeben sind, verbleibt die Sanktionskompetenz auch für direkt von der EZB beaufsichtigte Kreditinstitute oder (gemischte) Finanzholdinggesellschaften bei den nationalen Aufsichtsbehörden. Diese bringen nationale Sanktionsvorschriften und nationales Prozessrecht zur Anwendung. So keine Verpflichtung besteht, eine Sanktion zu verhängen, wird auch auf nationaler Ebene entschieden, ob, und in Folge in welcher Form und in welcher Höhe eine solche verhängt wird.

## IV. Schlussbemerkungen und Ausblick

Die Weiterentwicklung der Bankenaufsicht und insbesondere die Schaffung des Einheitlichen Bankenaufsichtsmechanismus sind als positive Beispiele dafür zu nennen, wie durch internationales Recht gemeinsame Interessen verwirklicht werden können. Im Bereich der Bankenaufsicht sind das die Förderung der Sicherheit und Solidität von Kreditinstituten, der Stabilität des Finanzsystems durch Sicherstellung hoher Aufsichtsstandards, die einheitlich angewendet werden und Aufsichtsarbitrage entgegenwirken. Durch die direkte und laufende Aufsicht von *significant institutions* durch gemeinsame Aufsichtsteams, die sich aus Experten/Expertinnen der EZB und

---

EuGH feststellte, dass diese als eine Maßnahme im Sinne des Art. 65 Abs. 1 CRD zu werten sind. Demnach kann die EZB diese gem. Art. 9 Abs. 1 SSM-Verordnung direkt anwenden. Siehe hierzu auch EuG, Urt. v. 28.2.2024 – Rs. T-667/21 (BAWAG PSK/EZB) – Rn. 23 ff.

[73] Nur nach Maßgabe des Art. 122 Abs. 2 SSM-Rahmenverordnung können nach Art. 18 Abs. 7 SSM-Verordnung auch gegenüber weniger bedeutenden beaufsichtigten Unternehmen Verwaltungsgeldbußen verhängt werden. Zur Beschränkung von Sanktionskompetenzen auf *significant institutions* siehe *Allegrezza/Voordeckers*, Investigative and Sanctioning Powers of the ECB in the Framework of the Single Supervisory Mechanism, eucrim 2015/4, 151 (156).

der nationalen Aufsichtsbehörden zusammensetzen, wird auch sichergestellt, dass Fachwissen und Sichtweisen länderübergreifend, und somit auch den länderübergreifenden Tätigkeiten von Kreditinstituten gerecht werdend, laufend ausgetauscht und angewendet werden, womit auch Risiken schneller erkannt und adressiert werden können.[74]

Im Hinblick auf Sanktionen im Einheitlichen Bankenaufsichtsmechanismus ist festzuhalten, dass dadurch, dass der EZB für von ihr direkt beaufsichtigte *significant institutions* beim Verstoß gegen einen einschlägigen direkt anwendbaren Rechtsakt der Union, z. B. eine Anforderung der CRR, und bei Verstößen gegen EZB-Beschlüsse und Verordnungen die Kompetenz eingeräumt wird, Verwaltungsgeldbußen zu verhängen, dem gemeinsamen Interesse von Rechtsicherheit auch in diesem Bereich Rechnung getragen wird. Dies, da zum einen eine konsistente Auslegung stattfindet, wann ein Verstoß gegeben ist, zum anderen, weil auch eine konsistente Reaktion bei Verstößen erfolgen kann, sowohl im Hinblick auf die Entscheidung, ob eine Sanktion verhängt wird oder eine andere Maßnahme ergriffen wird, als auch im Hinblick auf die Höhe der Verwaltungsgeldbuße.

Allerdings ist, wie festgestellt, die Kompetenz der EZB, Verwaltungsgeldbußen zu verhängen, beschränkt. Unter anderem, weil nach der SSM-Verordnung für eine EZB-Sanktionsmöglichkeit erforderlich ist, dass den zuständigen Behörden nach dem Unionsrecht wegen des Verstoßes gegen eine Anforderung aus direkt anwendbaren Rechtsakten der Union, wie der CRR, die Möglichkeit zur Verfügung gestellt wird, Verwaltungsgeldbußen zu verhängen. So dies nicht der Fall ist, weil z. B. in Art. 67 CRD, welcher vorgibt, bei welchen Verstößen Verwaltungssanktionen oder andere Verwaltungsmaßnahmen vorzusehen sind, der konkrete Verstoß nicht gelistet ist, und auch folgend national keine Sanktion vorgesehen ist, kann die EZB keine Verwaltungsgeldbuße nach Art. 18 Abs. 1 SSM-Verordnung verhängen. Positiv ist zu vermerken, dass die im Juli 2024 in Kraft getretene Änderung der CRD die Liste an Verstößen, in welchen Verwaltungssanktionen vorzusehen sind, ausgedehnt hat.[75] Sohin wird der Anwendungsbereich des Art. 18 Abs. 1 SSM-Verordnung auf weitere Verstöße erweitert und damit ebenso die Möglichkeit für die EZB, für eine größere Anzahl an Verstößen für eine einheitliche Reaktion zu sorgen. Allerdings handelt es sich weiterhin nur um einen Mindestkatalog. Außer dieser einschränkenden Voraussetzung für eine Verwaltungsgeldbuße durch die EZB verbleibt auch für all jene Fälle, in welchen gegen nationales Recht verstoßen wird, natürliche Personen belangt werden oder eine andere Sanktionsreaktion als eine Verwaltungsgeldbuße erfolgen soll, das Verfahren in jedem Fall bei den nationalen Behörden. Gem. Art. 134 SSM-Rahmenverordnung ist zwar sichergestellt, dass nationale zuständige Behörden nur auf Ersuchen der EZB ein Sanktionsverfahren gegen direkt von der EZB beaufsich-

[74] Siehe eine positive Einschätzung zum SSM im Bericht der Kommission an das Europäische Parlament und den Rat über den durch die Verordnung (EU) Nr. 1024/2013 geschaffenen einheitlichen Aufsichtsmechanismus, Straßburg, den 18.4.2023, COM(2023) 212 final.

[75] Art. 1 Abs. 1 Z. 17 zu Art. 67 Richtlinie (EU) 2024/1619, ErwGr. 34.

tigte *significant institutions* einleiten können, und damit ist eine gewisse Steuerung durch die EZB gegeben, bei welchen Verstößen eine Sanktion potentiell verhängt wird, aber das Verfahren und die Entscheidung, ob und welche Sanktion verhängt wird und über deren Ausmaß, obliegt der national zuständigen Behörde. Die EZB wird nur gem. Art. 134 Abs. 3 SSM-Rahmenverordnung über den Abschluss des Verfahrens und die verhängte Sanktion informiert. Potentiell gleich gelagerte Sachverhalte können sohin, trotz direkter Aufsicht durch die EZB, zu unterschiedlichen Ergebnissen in verschiedenen Ländern, die am SSM teilnehmen, führen. Dies kann z. B. bereits dann der Fall sein, wenn in einem Land Sanktionen verpflichtend für gewisse Verstöße zu verhängen sind, während in einem anderen Land, wie in Art. 18 Abs. 1 SSM-Verordnung, das Opportunitätsprinzip vorgesehen ist. Auch die nationale Praxis bei der Sanktionshöhe kann sich unterscheiden. Eine Vereinheitlichung ist diesbezüglich nicht erreicht. Nach Meinung des Autors wäre eine Ausweitung der Sanktionskompetenzen der EZB bei den von ihr direkt beaufsichtigen *significant institutions* ein Fortschritt, um eine Gleichbehandlung von gleichgelagerten Fällen auf europäischer Ebene sicherzustellen. Bei *less significant institutions*, die von den nationalen zuständigen Aufsichtsbehörden direkt beaufsichtigt werden, blieben potentielle Unterschiede weiterhin bestehen. Im Hinblick auf die bisherige Sanktionstätigkeit innerhalb des SSM ist auch auf die Veröffentlichungen auf der EZB-Homepage zu verweisen.[76]

Als Ausblick auf weitere Schritte zur Verwirklichung von gemeinsamen Interessen durch das Recht im Bereich der Aufsicht über Banken ist die Schaffung der *Anti Money Laundering Authority* (AMLA)[77] zu nennen. Mit der AMLA wird durch die direkte Aufsicht über risikoreiche, grenzüberschreitend tätige Unternehmen sowie die Überprüfung und Koordinierung der nationalen Aufsichtsbehörden eine Harmonisierung der Aufsicht im Bereich der Geldwäscheprävention gewährleistet.[78] Es

---

[76] Siehe hierzu https://www.bankingsupervision.europa.eu/banking/sanctions/html/index.en.html (Abrufdatum: 25.7.2024). Zu den Veröffentlichungspflichten von verhängten Sanktionen siehe Art. 18 Abs. 6 SSM-Verordnung, Art. 132 SSM-Rahmenverordnung, sowie Art. 1a Verordnung (EG) Nr. 2532/98. Siehe auch *Hauss*, Administrative Pecuniary Penalties and measures within the Single Supervisory Mechanism, in: FS für Wolfgang Brandstetter, 2022, 527 (536). Zur Frage der Ausnahmen von der Veröffentlichungspflicht siehe EuG, Urt. v. 8.7.2020 – Rs. T-203/18 (VQ/EZB) – Rn. 69 ff. Das Gericht prüfte, ob die Schwere eines Verstoßes für die Prüfung, ob eine Ausnahme von der Veröffentlichungspflicht des Beschlusses, mit dem eine Verwaltungsgeldbuße auferlegt wird, relevant ist.

[77] Verordnung (EU) 2024/1620 des Europäischen Parlaments und des Rates vom 31. Mai 2024 zur Errichtung der Behörde zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung und zur Änderung der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010, ABl. L 90/1 vom 19.6.2024. In diesem Zusammenhang ist auch auf die Richtlinie (EU) 2024/1640 des Europäischen Parlaments und des Rates vom 31. Mai 2024 über die von den Mitgliedstaaten einzurichtenden Mechanismen zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung, zur Änderung der Richtlinie (EU) 2019/1937 und zur Änderung und Aufhebung der Richtlinie (EU) 2015/849, ABl. L 94/1 vom 19.6.2024 zu verweisen.

[78] Die Aufsicht über die Agenden in Bezug auf die Prävention von Geldwäsche und Terrorismus-

wird mit Spannung zu beobachten sein, wie insbesondere auch die der AMLA eingeräumten Sanktionsbefugnisse mit Leben gefüllt werden.

finanzierung war nicht der EZB übertragen worden, sondern verblieb bei den zuständigen nationalen Aufsehern.

# Videoverhandlung und Videobeweisaufnahme im österreichischen und europäischen Zivilverfahrensrecht

*Philipp Anzenberger*



## I. Einleitung

Selbstgestecktes Ziel der Ringvorlesung „Internationalisierung und Digitalisierung" war es unter anderem, „vor dem Hintergrund der europäischen Regelungswelle im Digitalen […] die Rolle des Rechts als Instrument zur Förderung des gesellschaftlichen Zusammenhalts und der Realisierung gemeinsamer Interessen im internationalen Kontext aus[zu]leuchten"[1]. Nun mag der digitale Innovationsdruck im justiziellen Bereich – verglichen mit der „rauen Wildbahn" des freien Markts – etwas weniger stark ausgeprägt sein,[2] aber auch hier hat sich in den letzten Jahren Erstaunliches getan: Der österreichische Zivilprozess kennt mittlerweile den digitalen Akt[3] sowie Möglichkeiten der Videoverhandlung, in anderen Staaten wurden schon Ver-

[1] Abrufbar unter https://www.uibk.ac.at/rewi/nachhaltigkeit-digitalisierung/veranstaltungen/copy_of_24.html (Abrufdatum: 9.1.2025).

[2] *Spitzer*, Die Digitalisierung des Prozesses am Beispiel der Videoverhandlung, in: FS für Elisabeth Lovrek, 2024, 725 (728 f.).

[3] Siehe zu diesem Thema etwa die Beiträge von *Sommer*, Die Zivilverfahrens-Novelle 2022: Erweiterte Digitalisierung in der Justiz und Effizienzsteigerung im Zivilverfahrensrecht, Zak 2022, 144; *Spiegel*, ZVN 2022: Digitalisierung im Zivilverfahren, ecolex 2022, 614; *Wagner*, Die unendliche Geschichte, RZ 2021, 177.

handlungen mittels *virtual reality* durchgeführt[4] und die möglichen Nutzungsformen künstlicher Intelligenz werfen auch im Zivilverfahrensrecht erste Schatten voraus (man denke etwa an die Diskussion über *robo judges*, die mit Hilfe künstlicher Intelligenz Urteile fällen könnten[5]). Der vorliegende Beitrag wird sich – als schriftliche Version des Eröffnungsvortrags dieser Ringvorlesung im Sommersemester 2024 – zwei Aspekten der „Digitalisierung des Zivilverfahrens", nämlich der Videobeweisaufnahme (Abschnitt II.) und der Videoverhandlung (Abschnitt III.) widmen. Denn in beiden Bereichen sieht sich der Rechtsanwender – angesichts der Revision der Europäischen Beweisaufnahmeverordnung sowie des Inkrafttretens der ZVN 2023 – mit einer veränderten Rechtslage konfrontiert; die folgenden Ausführungen dürfen insoweit (auch) als Update über die jüngsten Neuerungen verstanden werden.

## II. Videobeweisaufnahme

### *1. Allgemeines*

Zunächst eine begriffliche Vorbemerkung: Unter der (im folgenden Kapitel darzustellenden) „Videobeweisaufnahme" wird in weiterer Folge die *Vernehmung von Zeugen, Parteien sowie Sachverständigen mittels Videotechnologie* verstanden. Eine Aufnahme von Augenscheins- oder Urkundenbeweisen im Weg der Videotechnologie ist theoretisch zwar ebenfalls denkbar, in der österreichischen Rechtsordnung aber nicht vorgesehen (arg. § 277 öZPO: „Einvernahmen") und kann daher in weiterer Folge ausgeblendet werden.

Das österreichische Zivilprozessrecht kennt die Möglichkeit einer Videobeweisaufnahme bereits seit dem 1.1.2005; ihr Anwendungsbereich wurde in weiterer Folge aufgrund positiver Erfahrungen etappenweise ausgeweitet.[6] Auch die meisten übrigen europäischen Prozessordnungen enthalten mittlerweile Instrumente zur Beweisaufnahme per Videokonferenztechnologie.[7] Gewissermaßen als „Bindeglied" zwischen

---

[4] Zu Einsätzen in Kolumbien und im deutschen Strafverfahren etwa *Heetkamp*, Die VR-Revolution im Justizwesen, e-justice 2023, 16 (17 f.).

[5] Dazu etwa *Heinze*, Zivilprozessuale Beweisführung und künstliche Intelligenz, in: Althammer/Roth (Hrsg.), Prozessuales Denken und Künstliche Intelligenz, 2023, 59; *Huber*, Entscheidungsfindung im Zivilprozess durch künstliche Intelligenz, in: Althammer/Roth (Hrsg.), Prozessuales Denken und Künstliche Intelligenz, 2023, 43; *Paar*, Einsatz künstlicher Intelligenz in der Justiz. Eine Bestandaufnahme, ÖJZ 2021, 213.

[6] Für einen Überblick siehe etwa *Ent*, Videoverhandlungen nach der ZVN 2023 (Teil 1), RZ 2023, 284 (284 f.); *Fink*, Die Digitalisierung der Justiz. Schwerpunkte der Zivilverfahrens-Novelle 2021, in: Fink/Otti/Sommer (Hrsg.), Zukunft der zivilrechtlichen Streitbeilegung. 6. Grazer Tagung der Assistentinnen und Assistenten zum Zivilverfahrensrecht, 2022, 1 (14 f.); *Rechberger*, Die Anwendung moderner Technologien im österreichischen Zivilprozess, in: FS für Helmut Rüßmann, 2013, 733 (740); *Rechberger*, in: Fasching/Konecny (Hrsg.), Kommentar zu den Zivilprozessgesetzen III/1, 3. Aufl., 2017, § 277 ZPO Rn. 1.

[7] Siehe dazu etwa die Informationen der Mitgliedstaaten zur Verwendung von Videokonferenztechnologie bei der zivilgerichtlichen Beweisaufnahme, abrufbar unter: https://e-justice.europa.eu/

den einzelnen nationalstaatlichen Verfahrensordnungen sieht die (jüngst revidierte) Europäische Beweisaufnahmeverordnung (EuBVO) Voraussetzungen vor, unter welchen eine Videobeweisaufnahme durchgeführt werden kann, wenn sich die zu vernehmende Person in einem anderen Mitgliedstaat als das Prozessgericht aufhält. Das weiterhin in Kraft stehende HBÜ 1970 wurde im Rechtsverkehr zwischen den Mitgliedstaaten (mit Ausnahme Dänemarks; vgl. ErwGr. 38 EuBVO) mittlerweile weitgehend durch die EuBVO ersetzt und dient hier nur noch zur Lückenschließung;[8] auf eine genauere Darstellung kann an dieser Stelle daher verzichtet werden.

### *2. Nationaler Rechtsrahmen: § 277 öZPO*

#### *a) Entstehungsgeschichte*

Mit der ZVN 2004[9] beschloss der österreichische Gesetzgeber, die zuvor bereits im Strafverfahren erfolgreich eingesetzten[10] „technischen Einrichtungen zur Wort- und Bildübertragung" auch für das Zivilverfahren zur Einvernahme von Zeugen, Sachverständigen und Parteien nutzbar zu machen.[11] Hierzu schuf er die Bestimmung des § 91a GOG, wonach ein Gericht nunmehr auch in zivilgerichtlichen Verfahren nach Maßgabe der technischen Möglichkeiten und unter Berücksichtigung der Verfahrensökonomie statt der Einvernahme durch einen ersuchten Richter eine unmittelbare Beweisaufnahme unter Verwendung technischer Einrichtungen zur Wort- und Bildübertragung durchführen konnte. Diese Möglichkeit war zunächst als *fakultative Alternative zur Beweisaufnahme* durch einen ersuchten Richter konstruiert, wovon

---

39432/DE/taking_evidence_by_videoconference?init=true (Abrufdatum: 9.1.2025); siehe etwa für Deutschland: § 128a dZPO; für Estland: § 350 *Tsiviilkohtumenetluse seadustiku* (estnische Zivilprozessordnung); für Finnland: Kapitel 17 Abschnitt 52 *Oikeudenkäymiskaari* (finnische Zivilprozessordnung); für Griechenland: Griechisches Präsidialdekret 142/2013 und Art. 393 Abs. 3 der griechischen Zivilprozessordnung; für Irland: Civil Law and Criminal Law (Miscellaneous Provisions) Act 2020, Number 13 of 2020; für Italien: Art. 127 bis *codice di procedura civile* (italienische Zivilprozessordnung); für Kroatien: Art. 115 *Zakon o parničnom postupku* (kroatische Zivilprozessordnung); für Lettland: Art. 108 Abs. 1 und Art. 122 *Civilprocesa likums* (lettische Zivilprozessordnung); für Malta: Art. 622b Abs. 2 maltesische Gerichtsverfassungs- und Zivilprozessordnung (Kapitel 12 der maltesischen Gesetze); für Polen: Art. 151 Abs. 2 und Art. 235 Abs. 2 *Kodeks Postępowania Cywilnego* (polnische Zivilprozessordnung); für Portugal: Art. 456, Art. 486 Abs. 2 und Art. 502 *Código de Processo* (portugiesische Zivilprozessordnung); für die Slowakei: § 175 *Civilný sporový poriadok* (slowakische Zivilstreitordnung); für Spanien: Art. 177 *Ley de Enjuiciamiento Civil* (spanische Zivilprozessordnung) und Art. 229 *Ley Orgánica del Poder Judicial* (spanisches Gerichtsverfassungsgesetz); für Tschechien: § 102a *občanský soudní řád* (tschechische Zivilprozessordnung); für Ungarn: § 622 *A polgári perrendtartásról szóló 2016. évi CXXX. Törvény* (ungarische Zivilprozessordnung).

[8] Vgl. etwa *Labonté/Rohrbeck*, Grenzüberschreitende Beweisaufnahmen im Zivilprozess unter Einsatz von Fernkommunikationsmitteln, IWRZ 2021, 99 (99).

[9] BGBl. I 2004/128.

[10] Vgl. dazu etwa *Fink*, in: Fink/Otti/Sommer, Zukunft, 1 (14 f.); *Schmidt*, Vernehmungen mit Videokonferenztechnik, in: Fucik/Konecny/Lovrek/Oberhammer (Hrsg.), Zivilverfahrensrecht. Jahrbuch 2009, 2009, 167 (169).

[11] ErläutRV 613 BlgNR 22. GP 21.

das Verfahrensgericht nach seinem Ermessen (und zwar unter Berücksichtigung der Richtigkeit und Vollständigkeit des festzustellenden Sachverhalts auf der einen und – nach ausdrücklicher gesetzlicher Anordnung – der Verfahrensökonomie auf der anderen Seite[12]) Gebrauch machen konnte.[13]

Damit war zwar der Grundstein für den „Siegeszug" der Videoeinvernahme im österreichischen Zivilprozess gelegt, ihrer anfänglich teils eher zurückhaltenden Inanspruchnahme[14] musste allerdings erst Stück für Stück nachgeholfen werden: Zunächst überführte der Gesetzgeber mit der ZVN 2009[15] die Bestimmung in den § 277 öZPO, um die Sichtbarkeit der Möglichkeit von Videoeinvernahmen zu erhöhen und dadurch ihre Anwendung zu fördern.[16] Gleichzeitig wurde auch im AußStrG eine entsprechende Änderung vorgenommen und in § 35 AußStrG die Wortfolge „über die Verwendung technischer Einrichtungen zur Wort- und Bildübertragung bei der Beweisaufnahme" hinzugefügt. Dadurch gelangte § 277 öZPO sinngemäß auch im Außerstreitverfahren zur Anwendung.[17] Zudem verlor der (nach wie vor im Gesetzestext enthaltene) Vorbehalt der „Maßgabe der technischen Möglichkeiten" aufgrund der kontinuierlichen Verbesserung der technischen Ausstattung der Gerichte nach und nach an Bedeutung;[18] im Jahr 2011 waren bereits alle österreichischen Gerichte mit den notwendigen Anlagen ausgestattet.[19] Schließlich normierte der Gesetzgeber aufgrund weitgehend positiver Erfahrungen und Rückmeldungen[20] mit dem BudgetbegleitG 2011[21] einen Anwendungsvorrang der Videoeinvernahme vor einer Rechtshilfeeinvernahme: Hiervon kann das Gericht zu Gunsten einer Einvernahme durch einen beauftragten oder ersuchten Richter nur ausnahmsweise aus Gründen der Verfahrensökonomie oder aufgrund sonstiger besonderer Umstände (etwa der Notwendigkeit, eine nicht transportfähige Person zu Hause aufzusuchen[22]) abweichen. Mittlerweile hat sich die Einvernahme im Weg der Videokonferenz in der Praxis vollkommen etabliert[23] und zählt zum Standardrepertoire der zivilgerichtlichen Verfahrensführung.

---

[12] ErläutRV 613 BlgNR 22. GP 21.

[13] ErläutRV 613 BlgNR 22. GP 21.

[14] Etwa *Schmidt*, in: Fucik/Konecny/Lovrek/Oberhammer, Zivilverfahrensrecht. Jahrbuch 2009, 167 (176 f.); *Schmidt*, Videokonferenztechnologie statt Rechtshilfe, RZ 2006, 265 (267); vgl. auch die Ausführungen von *Schmidbauer/Illyes*, Medieneinsatz bei der richterlichen Arbeit, in: Bundesministerium für Justiz (Hrsg.), Die Medienlandschaft 2015. Herausforderungen für die Justiz, 2016, 113 (119 ff.).

[15] BGBl. I 2009/30.

[16] ErläutRV 89 BlgNR 24. GP 14; vgl. auch *Ent*, RZ 2023, 284 (285).

[17] ErläutRV 89 BlgNR 24. GP 26.

[18] ErläutRV 981 BlgNR 24. GP 85.

[19] *Rechberger*, in: Fasching/Konecny, Kommentar III/1, 3. Aufl., 2017, § 277 ZPO Rn. 1; *Rechberger*, in: FS für Helmut Rüßmann, 733 (743); *Sengstschmid*, Videokonferenz und Öffentlichkeit. Die Wahrung der Öffentlichkeit bei audiovisuellen Verhandlungen in Zivilverfahren, in: FS für Andreas Konecny, 2022, 553 (554).

[20] ErläutRV 981 BlgNR 24. GP 85.

[21] BGBl. I 2010/111.

[22] ErläutRV 981 BlgNR 24. GP 86.

[23] *Rechberger*, in: Fasching/Konecny, Kommentar III/1, 3. Aufl., 2017, § 277 ZPO Rn. 1; *Spitzer*,

*b) Anwendungsvoraussetzungen*

*aa) Maßgebliche Bestimmungen*

Aus der in § 277 öZPO gewählten Wortfolge „statt der Einvernahme durch einen ersuchten Richter" ergibt sich, dass die Voraussetzungen für eine Vernehmung im Rechtshilfeweg auch für die Durchführung einer Videobeweisaufnahme gelten.[24] Insoweit ist für die Einvernahme von Zeugen auf die Kriterien des § 328 Abs. 1 öZPO, für die Aufnahme des Sachverständigenbeweises auf § 352 Abs. 1 öZPO bzw. für die Einvernahme von Parteien auf die Voraussetzungen des § 375 Abs. 2 öZPO abzustellen.

Bereits eingangs zu klären ist in diesem Zusammenhang, ob die Anwendungsvoraussetzungen für die Videoeinvernahme tatsächlich deckungsgleich zu jenen sind, welche für die Vernehmung durch einen ersuchten Richter gelten. Zumindest nach Teilen des Schrifttums[25] soll hier ein großzügigerer Maßstab anzulegen sein, zumal es sich bei der Videoeinvernahme bereits *expressis verbis*[26] um eine unmittelbare Beweisaufnahme handle.[27] Andere Teile des Schrifttums vertreten demgegenüber, dass die Beweisaufnahme im Weg der Videokonferenz ein Substitut für die Beweisaufnahme im Rechtshilfeweg darstelle, weshalb die Anwendungsvoraussetzungen für die Inanspruchnahme eines ersuchten Richters weiterhin gegeben sein müssten.[28] Konkrete Auswirkungen kann das etwa bei § 328 Abs. 1 Z. 3 öZPO („unverhältnismäßig großer Aufwand der Vernehmung vor dem erkennenden Gericht") haben,[29] weil in die notwendige Verhältnismäßigkeitsprüfung bei Vernehmung durch einen ersuchten Richter auch die Mehrkosten der Parteien für eine Teilnahme an einer

---

in: Kodek/Oberhammer (Hrsg.), ZPO-ON, 2023, § 277 ZPO Rn. 1; *Spitzer*, in: Spitzer/Wilfinger (Hrsg.), Beweisrecht. Kommentar der §§ 266 bis 389 ZPO, 2020, § 277 ZPO Rn. 1.

[24] Insoweit ausdrücklich etwa ErläutRV 981 BlgNR 24. GP 85; ebenso *Oberhammer/Scholz-Berger*, Möglichkeiten und Grenzen der Videoeinvernahme nach § 277 ZPO, ecolex 2022, 285 (286); *Spitzer*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 277 ZPO Rn. 3; *Spitzer*, in: Spitzer/Wilfinger, Beweisrecht, 2020, § 277 ZPO Rn. 3.

[25] *Oberhammer/Scholz-Berger*, ecolex 2022, 285 (286); in diese Richtung wohl auch *Frauenberger*, in: Fasching/Konecny, Kommentar III/1, 3. Aufl., 2017, § 328 ZPO Rn. 6/1.

[26] Kritisch dazu *Rechberger*, in: Fasching/Konecny, Kommentar III/1, 3. Aufl., 2017, § 277 ZPO Rn. 2; *Rechberger/Klicka*, in: Rechberger/Klicka (Hrsg.), ZPO. Zivilprozessordnung, 5. Aufl., 2019, § 277 ZPO Rn. 2.

[27] *Oberhammer/Scholz-Berger*, ecolex 2022, 285 (286); ähnlich *Spitzer*, in: Spitzer/Wilfinger, Beweisrecht, 2020, § 277 ZPO Rn. 3, der aber auch festhält, dass die Beweisaufnahme durch Videokonferenz nur zulässig sei, wenn die Voraussetzungen für die Einvernahme durch einen ersuchten Richter vorliegen würden.

[28] *Fucik*, Rechtsentwicklung 2010/11, in: Fucik/Konecny/Oberhammer (Hrsg.), Zivilverfahrensrecht. Jahrbuch 2011, 2011, 9 (27 f.); *Rechberger*, in: Fasching/Konecny, Kommentar III/1, 3. Aufl., 2017, § 277 ZPO Rn. 2; *Rechberger*, in: FS für Helmut Rüßmann, 733 (745); *Rechberger/Klicka*, in: Rechberger/Klicka, ZPO, 5. Aufl., 2019, § 277 ZPO Rn. 2; ebenso *Spitzer*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 277 ZPO Rn. 3; wohl auch *Spitzer*, in: Spitzer/Wilfinger, Beweisrecht, 2020, § 277 ZPO Rn. 3.

[29] So schon *Oberhammer/Scholz-Berger*, ecolex 2022, 285 (286).

auswärtigen Beweisaufnahmetagsatzung einzubeziehen sind[30] und diese bei der Videoeinvernahme nicht anfallen.

Die Annahme „großzügigerer Anwendungsvoraussetzungen" des § 277 öZPO im Verhältnis zu § 328 Abs. 1, § 352 Abs. 1 und § 375 öZPO mag *prima vista* praxisfreundlich wirken, bei genauerer Betrachtung tauchen allerdings gewisse Zweifel an dieser Sichtweise auf: Bereits der Wortlaut des § 277 öZPO (arg.: „statt der Einvernahme durch einen ersuchten Richter") legt nahe, dass die Voraussetzungen für die Beweisaufnahme durch einen ersuchten Richter weiterhin vorliegen müssen, um eine Videoeinvernahme anordnen zu können. Dieser Verdacht erhärtet sich bei Betrachtung der „Rückausnahme" („es sei denn, die Einvernahme durch einen beauftragten oder ersuchten Richter ist unter Berücksichtigung der Verfahrensökonomie zweckmäßiger oder aus besonderen Gründen erforderlich"), die ja nur praktikabel ist, wenn die Anwendungsvoraussetzungen für die Rechtshilfeeinvernahme vorliegen. Unklar wäre in diesem Zusammenhang auch, wie die „sinngemäße Anwendung" der § 328 Abs. 1, § 352 Abs. 1 und § 375 öZPO „technisch" funktionieren soll: Eine direkte Anwendung scheitert hier nämlich wohl an deren Wortlautgrenze; eine analoge Anwendung (wohl des § 277 öZPO auf jene Sachverhalte, welche nicht von § 328 Abs. 1, § 352 Abs. 1 und § 375 öZPO erfasst sind) hingegen an der Planwidrigkeit dieser Nichtregelung, wie die entsprechenden Gesetzesmaterialien zeigen:[31] Schon die Erläuterungen zur ZVN 2004 legen den Eindruck nahe, dass es sich bei der Videobeweisaufnahme um eine *alternative Erledigungsform* all jener Beweisaufnahmen handeln solle, welche andernfalls durch einen ersuchten Richter durchgeführt werden müssten. So weist der Gesetzgeber etwa darauf hin, dass diese Form der Einvernahme in aller Regel Vorteile biete, etwa weil die Notwendigkeit der Verfassung eines Rechtshilfeersuchens entfalle und auch der Akt nicht an das Rechtshilfegericht übersendet werden müsse.[32] Besonders explizit sind die Materialien zum BudgetbegleitG 2011: Dort wird festgehalten, dass die Videoeinvernahme „unter den gleichen Voraussetzungen (§ 328 Abs. 1; arg.: ‚statt') durchgeführt"[33] werden könne wie die Einvernahme durch einen ersuchten Richter. Sie komme nach wie vor nur dann in Betracht, „wenn die Voraussetzungen des Einsatzes eines ersuchten Richters vorliegen und die technischen Möglichkeiten vorhanden sind."[34] Zuzugestehen ist freilich, dass die Gesetzestechnik hier wenig glücklich ist[35] und dass es auch etwas befremdlich wirkt, die Zulässigkeit einer Videoeinvernahme anhand der Kriterien einer (ohnehin nie geplanten) Einvernahme im Rechtshilfeweg zu messen. Umgekehrt könnte allerdings eine Abkehr von den (strengen) Voraussetzungen der Rechts-

---

[30] Vgl. *Frauenberger*, in: Fasching/Konecny, Kommentar III/1, 3. Aufl., 2017, § 328 ZPO Rn. 6.
[31] Vgl. schon *Rechberger*, in: FS für Helmut Rüßmann, 733 (745).
[32] ErläutRV 613 BlgNR 22. GP 21.
[33] ErläutRV 981 BlgNR 24. GP 85.
[34] ErläutRV 981 BlgNR 24. GP 85.
[35] So schon *Fucik*, in: Fucik/Konecny/Oberhammer, Zivilverfahrensrecht. Jahrbuch 2011, 9 (27), der von einem „Konstruktionsfehler" spricht.

hilfeeinvernahme den Grundsatz der Unmittelbarkeit nicht unerheblich verwässern: Denn gerade bei § 328 Abs. 1 Z. 3 öZPO („unverhältnismäßig großer Aufwand der Vernehmung vor dem erkennenden Gericht") würde die in einem ersten Schritt notwendige Vergleichsrechnung (Zeugengebühren bei dessen Erscheinen vor dem Prozessgericht versus Mehrkosten der Parteien bei „auswärtiger" Einvernahme)[36] bei einer Videoeinvernahme wohl fast immer zu deren Gunsten ausgehen. In einem zweiten Schritt sind die voraussichtlichen Zeugengebühren an der wirtschaftlichen Bedeutung des Streitgegenstands zu messen.[37] Konkret würde das gerade bei geringen Streitwerten bedeuten, dass das Gericht zahlreiche Zeugenvernehmungen gem. § 277 öZPO durchführen könnte, und zwar auch gegen den (allenfalls übereinstimmenden) Willen der Parteien. Eine solche „Herabsetzung" der Unmittelbarkeit zugunsten der Verfahrensökonomie kann man rechtspolitisch für wünschenswert erachten,[38] sie entspricht (derzeit) aber nicht dem Willen des Gesetzgebers.[39]

*bb) Konkrete Anwendungsvoraussetzungen*

Aufgrund des Verweises in § 277 öZPO ist die *Videoeinvernahme von Zeugen* in den Fällen des § 328 Abs. 1 öZPO zulässig, wobei die Z. 1 (Vernehmung des Zeugen an Ort und Stelle erscheint der Ermittlung der Wahrheit förderlich) wohl in aller Regel eine tatsächliche Beweisaufnahme im Rechtshilfeweg indiziert. Nach Z. 2 ist eine Videovernehmung dann zulässig, wenn die Beweisaufnahme vor dem erkennenden Gericht erheblichen Schwierigkeiten unterliegen würde, was in der Entscheidung OGH 6 Ob 14/64 etwa im Fall eines Strafgefangenen bejaht wurde, der vor ein weit entferntes Prozessgericht gebracht hätte werden müssen.[40] Gem. Z. 3 kann eine Videoeinvernahme auch dann erfolgen, wenn die Vernehmung des Zeugen vor dem erkennenden Gericht mit Rücksicht auf die dem Zeugen zu gewährende Entschädigung für Zeitversäumnis und die ihm zu erstattenden Kosten der Reise und des Aufenthalts am Ort der Vernehmung einen unverhältnismäßig großen Aufwand verursachen würde. Und schließlich ist eine Vorgangsweise nach § 277 öZPO dann möglich, wenn der Zeuge an dem Erscheinen vor dem erkennenden Gericht gehindert ist (Z. 4). Dies wird von der zutreffenden herrschenden Auffassung nicht erst bei „physischer Unmöglichkeit", sondern bereits bei Unzumutbarkeit, etwa aufgrund des Gesundheitszustands, beruflicher Verpflichtungen oder unabkömmlicher Pflegeaufgaben angenommen.[41] Dem soll es nach überzeugender Auffassung von *Oberhammer/Scholz-Berger*[42] auch gleichzuhalten sein, wenn ein im Ausland aufhältiger Zeuge

---

[36] *Frauenberger*, in: Fasching/Konecny, Kommentar III/1, 3. Aufl., 2017, § 328 ZPO Rn. 6.
[37] *Frauenberger*, in: Fasching/Konecny, Kommentar III/1, 3. Aufl., 2017, § 328 ZPO Rn. 6.
[38] So etwa *Ent*, Videoverhandlungen nach der ZVN 2023 (Teil 2), RZ 2024, 56 (59).
[39] Vgl. auch *Fucik*, in: Fucik/Konecny/Oberhammer, Zivilverfahrensrecht. Jahrbuch 2011, 9 (28).
[40] *Frauenberger*, in: Fasching/Konecny, Kommentar III/1, 3. Aufl., 2017, § 328 ZPO Rn. 5.
[41] *Oberhammer/Scholz-Berger*, ecolex 2022, 285 (286).
[42] *Oberhammer/Scholz-Berger*, ecolex 2022, 285 (286).

zwar grundsätzlich zur Aussage bereit ist, allerdings eine Anreise nach Österreich ablehnt (zumindest, soweit ihn – was ja den Regelfall darstellt – keine Pflicht zum Erscheinen vor Gericht trifft).

Die *Aufnahme des Sachverständigenbeweises* mittels Videotechnologie war bis vor kurzem nur über § 277 i. V. m. § 352 Abs. 1 öZPO zulässig: Nach § 352 Abs. 1 öZPO kann die Aufnahme eines Sachverständigenbeweises durch einen beauftragten oder ersuchten Richter erfolgen, wenn ein durch Sachverständige zu besichtigender Gegenstand nicht vor das erkennende Gericht gebracht werden kann oder die Aufnahme des Sachverständigenbeweises vor demselben aus anderen Gründen erheblichen Schwierigkeiten unterliegen würde. Diese etwas antiquierte Bestimmung erklärt sich damit, dass der Sachverständigenbeweis nach dem Konzept der öZPO an sich mündlich zu erstatten ist;[43] aufgrund der in der Praxis überwiegend schriftlich erfolgenden Begutachtung kam der mündlichen Erstattung aber bereits vor Inkrafttreten der ZVN 2023 kaum praktische Bedeutung zu.[44] Nunmehr kann die mündliche Erstattung sowie die Erörterung von Sachverständigengutachten gem. § 132a Abs. 1 öZPO sogar ohne die Voraussetzungen des § 277 öZPO mittels Videotechnologie durchgeführt werden.[45] Ein (etwa mangels Zustimmung der Parteien zu einem solchen Vorgehen weiterhin denkbarer; vgl. dazu Abschnitt III.2.b) Rückgriff auf § 277 i. V. m. § 352 Abs. 1 öZPO wird daher in aller Regel nicht notwendig sein.

Eine *Einvernahme der Parteien* per Videotechnologie ist über die Bestimmung des § 277 öZPO (zur Ausnahme in § 132a öZPO siehe noch in Abschnitt III.2.c) nur eingeschränkt möglich: Denn § 375 Abs. 2 öZPO sieht eine entsprechende Beweisaufnahme durch einen ersuchten Richter nur dann vor, wenn dem persönlichen Erscheinen der Partei unübersteigliche Hindernisse entgegenstehen oder dieses unverhältnismäßige Kosten verursachen würde. Die Ausführungen des Schrifttums zur konkreten Auslegung dieser beiden Tatbestandsmerkmale sind eher karg; nach der Rechtsprechung soll die Parteieneinvernahme per Videokonferenz nur ausnahmsweise zulässig sein.[46] Nach herrschender Auffassung ist die Formulierung „unübersteigliches Hindernis“ parallel zu § 134 Z. 1 öZPO auszulegen;[47] dabei sei zu überprüfen, ob der Partei ihr persönliches Erscheinen in Anbetracht ihrer konkreten Umstände zugemutet werden kann.[48] Dies könne bei einer im Ausland aufhältigen Partei etwa dann zu verneinen sein, wenn sie einer strafrechtlichen Verfolgung im Inland ausgesetzt sei.[49]

---

[43] *Schneider*, in: Fasching/Konecny, Kommentar III/1, 3. Aufl., 2017, § 352 ZPO Rn. 2.

[44] *Schneider*, in: Fasching/Konecny, Kommentar III/1, 3. Aufl., 2017, § 352 ZPO Rn. 2.

[45] *Ent*, RZ 2024, 56 (56).

[46] OLG Wien 7.7.2023, 3 R 149/22m; RIS-Justiz RW0001032.

[47] OLG Wien 7.7.2023, 3 R 149/22m; *Oberhammer/Scholz-Berger*, ecolex 2022, 285 (287); *Rechberger/Klicka*, in: Rechberger/Klicka, ZPO, 5. Aufl., 2019, § 375 ZPO Rn. 3; *Spenling*, in: Fasching/Konecny, Kommentar III/1, 3. Aufl., 2017, § 375 ZPO Rn. 10.

[48] OLG Wien 7.7.2023, 3 R 149/22m; *Oberhammer/Scholz-Berger*, ecolex 2022, 285 (287).

[49] *Oberhammer/Scholz-Berger*, ecolex 2022, 285 (287).

Voraussetzung für die Durchführung einer Videoeinvernahme ist schließlich, dass die *technischen Voraussetzungen* dafür vorhanden sind, was in Österreich seit 2011 flächendeckend der Fall ist.[50] Allerdings ist der Anwendungsbereich des § 277 öZPO nicht auf im Inland zu vernehmende Personen beschränkt,[51] sodass diesem Tatbestandsmerkmal auch praktisch weiterhin Bedeutung zukommen kann. Die Durchführung einer Videoeinvernahme ist von der *Zustimmung der Parteien unabhängig.*[52] Soweit die Anwendungsvoraussetzungen nicht vorliegen, können diese nach herrschender Auffassung allerdings durch eine solche Zustimmung ersetzt werden.[53]

*c) Rechtsfolge*

Ist der Anwendungsbereich von § 328 Abs. 1, § 352 Abs. 1 oder § 375 Abs. 2 öZPO eröffnet, so hat das Gericht nach dem Wortlaut dieser Bestimmungen die Möglichkeit (aber nicht die Verpflichtung), an Stelle einer unmittelbaren Einvernahme des Zeugen, des Sachverständigen oder der Partei diese durch einen beauftragten oder ersuchten Richter vornehmen zu lassen. Aus § 277 öZPO ergibt sich in diesen Fällen ein *Vorrang der Videoeinvernahme,*[54] sofern die Einvernahme durch einen beauftragten oder ersuchten Richter nicht unter Berücksichtigung der Verfahrensökonomie zweckmäßiger oder aus besonderen Gründen erforderlich ist. In diese Beurteilung sind nach den Gesetzesmaterialien auch die Auswirkungen auf die Raschheit des Verfahrens, die materielle Wahrheitsfindung sowie die Verfahrenskosten einzubeziehen.[55] Gegen die Zweckmäßigkeit einer Videoeinvernahme könnten umfangreiche Vorhalte von Urkunden und physischen Augenscheinsgegenständen oder die Notwendigkeit, eine nicht transportfähige Person zu Hause aufzusuchen, sprechen.[56] Die Beurteilung der Zweckmäßigkeit einer Einvernahme durch einen ersuchten Richter liegt im Ermessen des Verfahrensgerichts.[57]

Bedient sich das Gericht einer mittelbareren Art der Beweisaufnahme als vorgesehen (also erachtet es irrtümlich die Anwendungsbereiche der § 328 Abs. 1, 352 Abs. 1 oder § 375 Abs. 2 öZPO für eröffnet oder nimmt es fälschlich eine der Gegenausnah-

---

[50] *Rechberger*, in: Fasching/Konecny, Kommentar III/1, 3. Aufl., 2017, § 277 ZPO Rn. 1; *Rechberger*, in: FS für Helmut Rüßmann, 733 (743).

[51] *Oberhammer/Scholz-Berger*, ecolex 2022, 285 (286); *Rechberger*, in: Fasching/Konecny, Kommentar III/1, 3. Aufl., 2017, § 277 ZPO Rn. 1; *Rechberger/Klicka*, in: Rechberger/Klicka, ZPO, 5. Aufl., 2019, § 277 ZPO Rn. 1.

[52] *Oberhammer/Scholz-Berger*, ecolex 2022, 285 (286).

[53] *Ent*, RZ 2024, 56 (59); *Oberhammer/Scholz-Berger*, ecolex 2022, 285 (288).

[54] *Rechberger*, in: Fasching/Konecny, Kommentar III/1, 3. Aufl., 2017, § 277 ZPO Rn. 1; *Rechberger*, in: FS für Helmut Rüßmann, 733 (741); *Spitzer*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 277 ZPO Rn. 1; *Spitzer*, in: Spitzer/Wilfinger, Beweisrecht, 2020, § 277 ZPO Rn. 1.

[55] ErläutRV 981 BlgNR 24. GP 85; vgl. auch *Obermaier*, in: Höllwerth/Ziehensack (Hrsg.), ZPO. Taschenkommentar, 2019, § 277 ZPO Rn. 1.

[56] ErläutRV 981 BlgNR 24. GP 85; vgl. auch *Obermaier*, in: Höllwerth/Ziehensack, ZPO, 2019, § 277 ZPO Rn. 1.

[57] *Rechberger*, in: Fasching/Konecny, Kommentar III/1, 3. Aufl., 2017, § 277 ZPO Rn. 1.

men des § 277 öZPO an), so stellt dies einen Verstoß gegen den Unmittelbarkeitsgrundsatz dar, der im Rechtsmittel als wesentlicher Verfahrensmangel geltend gemacht werden kann.[58] Ob ein solcher Verstoß von den Parteien gem. § 196 öZPO gerügt werden muss, ist im Schrifttum umstritten,[59] wird von der ständigen Rechtsprechung allerdings bejaht.[60]

### *3. Europäischer Rechtsrahmen: EuBVO*

#### *a) Allgemeines zur EuBVO*

Im folgenden Abschnitt sollen die Rahmenbedingungen für die Videobeweisaufnahme im grenzüberschreitenden Rechtsverkehr dargestellt und dabei insbesondere auf die einschlägigen Regeln der jüngst revidierten EuBVO eingegangen werden. Die Möglichkeit eines Rechtshilfeersuchens an ausländische Gerichte zum Zweck der Beweisaufnahme durch diese Gerichte („aktive Rechtshilfe") ergibt sich bereits aus § 36 JN i. V. m. §§ 300, 328, 352, 368 und 375 öZPO. Der nationale Rahmen für die Beweisaufnahme eines österreichischen Gerichts im Ausland („passive Rechtshilfe") ist in den §§ 291a ff. öZPO normiert, wohingegen die umgekehrte Situation (also eine Beweisaufnahme ausländischer Gerichte in Österreich) in den §§ 38 ff. JN geregelt ist.[61]

Die EuBVO legt – insoweit als Bindeglied zwischen den einzelnen nationalstaatlichen Verfahrensordnungen – die Modalitäten für die Gewährung von aktiver und passiver Rechtshilfe bei der Beweisaufnahme im Ausland fest; ihre kürzlich revidierte Fassung ist (im Wesentlichen[62]) seit 1.7.2022 in Geltung. Neu sind dabei insbesondere ausführliche Bestimmungen über die unmittelbare Beweisaufnahme per Videokonferenz oder anderer Fernkommunikationstechnologien (Art. 20 EuBVO) sowie gewisse Modifikationen der Beweisaufnahme durch das ersuchte Gericht in

---

[58] OLG Wien 7.7.2023, 3 R 149/22m; *Rechberger*, in: Fasching/Konecny, Kommentar III/1, 3. Aufl., 2017, Vor § 266 ZPO Rn. 90 und § 277 ZPO Rn. 2; *Rechberger/Klicka*, in: Rechberger/Klicka, ZPO, 5. Aufl., 2019, § 277 ZPO Rn. 2; (offenlassend hingegen noch *Rechberger*, in: FS für Helmut Rüßmann, 733 [746]); *Schneider*, in: Fasching/Konecny, Kommentar III/1, 3. Aufl., 2017, § 352 ZPO Rn. 1; *Spitzer*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 277 ZPO Rn. 4; *Spitzer*, in: Spitzer/Wilfinger, Beweisrecht, 2020, § 277 ZPO Rn. 4.

[59] Dafür etwa *Fasching*, Kommentar III, 1. Aufl., 1966, 484; *Fasching*, Zivilprozessrecht: Lehr- und Handbuch des österreichischen Zivilprozessrechts, 2. Aufl., 1990, Rn. 676; *Höllwerth*, in: Fasching/Konecny, Kommentar II/3, 3. Aufl., 2015, § 196 ZPO Rn. 14; *Trenker*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 196 ZPO Rn. 8; *Trenker*, Zum Anwendungsbereich der Rügelast nach § 196 ZPO, JBl 2020, 352 (359 f.); *Ziehensack*, in: Höllwerth/Ziehensack, ZPO, 2019, § 196 ZPO Rn. 3; dagegen *Bajons*, in: FS für Hans Fasching, 1988, 19 (32); *Rechberger*, in: Fasching/Konecny, Kommentar III/1, 3. Aufl., 2017, Vor § 266 ZPO Rn. 90; *Rechberger/Simotta*, Grundriss des österreichischen Zivilprozessrechts. Erkenntnisverfahren, 9. Aufl., 2017, Rn. 805.

[60] Etwa OGH 14.10.1993, 8 Ob 578/93; 1.12.1999, 9 ObA 222/99h; zuletzt 27.9.2023, 9 ObA 63/23i; vgl. auch RIS-Justiz RS0037410.

[61] Vgl. ausführlich *Fucik*, in: Fasching/Konecny, Kommentar III/1, 3. Aufl., 2017, § 291a ZPO Rn. 4.

[62] Zu den Ausnahmen siehe Art. 35 EuBVO.

Bezug auf ein Ersuchen der Verwendung solcher Technologien (Art. 12 Abs. 4 EuBVO). Weitere Neuerungen betreffen die Regelung der diplomatischen und konsularischen Beweisaufnahme im Ausland (Art. 21 EuBVO), die Verwendung von IT-Systemen bei der Übermittlung von Ersuchen und Mitteilungen (Art. 7 EuBVO) sowie die Rechtswirkungen elektronischer Schriftstücke (Art. 8 EuBVO).

*b) Videoeinvernahme durch das ersuchte Gericht („aktive Rechtshilfe")*

Die Beweisaufnahme durch das ersuchte Gericht ist in Art. 12 ff. EuBVO geregelt; diese Bestimmungen kommen etwa dann zur Anwendung, wenn ein österreichisches Gericht gem. § 277 i. V. m. § 328 Abs. 1, § 352 Abs. 1 oder § 375 Abs. 2 öZPO eine Beweisaufnahme durch einen ersuchten Richter durchführen möchte und die zu vernehmende Person in einem anderen Mitgliedstaat aufhältig ist.[63]

Gem. Art. 12 Abs. 4 UAbs. 1 EuBVO kann das ersuchende Gericht das ersuchte Gericht bitten, die begehrte Beweisaufnahme unter Verwendung einer besonderen Kommunikationstechnologie, insbesondere im Weg der Videokonferenz oder Telekonferenz, durchzuführen.[64] Dem hat das ersuchte Gericht gem. UAbs. 2 grundsätzlich zu entsprechen, sofern dies nicht ausnahmsweise mit seinem nationalen Recht unvereinbar oder wegen erheblicher tatsächlicher Schwierigkeiten unmöglich ist (davon wäre das ersuchende Gericht gem. UAbs. 3 mittels eines Formblatts zu unterrichten).[65] Fehlen dem ersuchenden oder dem ersuchten Gericht die entsprechenden Technologien, so können diese gem. UAbs. 4 im Einvernehmen zur Verfügung gestellt werden.[66] Die Beweisaufnahme durch ein ersuchtes Gericht kann (vorbehaltlich der Vereinbarkeit mit dem Recht des Mitgliedstaats des ersuchten Gerichts) in Anwesenheit und unter Beteiligung der Parteien (Art. 13 EuBVO) und des ersuchenden Gerichts (Art. 14 EuBVO) erfolgen. Dies macht die Verwendung von Videotechnologie auch bei aktiver Rechtshilfe durchaus attraktiv, zumal das Gericht und die Parteien auf diese Weise einfach und kostengünstig der Einvernahme beiwohnen (und sich allenfalls sogar daran beteiligen) können.[67] Freilich wendet das ersuchte

---

[63] *Sengstschmied*, in: Mayr (Hrsg.), Handbuch des europäischen Zivilverfahrensrechts, 2. Aufl., 2023, Rn. 15.52.

[64] *Mosser*, in: Fasching/Konecny, Kommentar V/3, 3. Aufl., 2023, Art. 12 EuBVO 2020 Rn. 24; *Rauscher*, in: Krüger/Rauscher (Hrsg.), Münchener Kommentar zur Zivilprozessordnung III, 6. Aufl., 2022, Art. 10 EG-BewVO Rn. 13; *Sengstschmied*, in: Mayr, Handbuch, 2. Aufl., 2023, Rn. 15.176.

[65] *Mosser*, in: Fasching/Konecny, Kommentar V/3, 3. Aufl., 2023, Art. 12 EuBVO 2020 Rn. 27; *Rauscher*, in: Krüger/Rauscher, MünchKommZPO III, 6. Aufl., 2022, Art. 10 EG-BewVO Rn. 13; *Sengstschmied*, in: Mayr, Handbuch, 2. Aufl., 2023, Rn. 15.176.

[66] *Mosser*, in: Fasching/Konecny, Kommentar V/3, 3. Aufl., 2023, Art. 12 EuBVO 2020 Rn. 27; *Rauscher*, in: Krüger/Rauscher, MünchKommZPO III, 6. Aufl., 2022, Art. 10 EG-BewVO Rn. 14; *Sengstschmied*, in: Mayr, Handbuch, 2. Aufl., 2023, Rn. 15.177.

[67] Dazu auch *Kohake*, Grenzüberschreitende Beweisaufnahme per Video? DRiZ 2021, 378 (381); vgl. auch *Fabig/Windau*, Die Neufassungen der Europäischen Zustellungs- und Beweisaufnahmeverordnungen, NJW 2022, 1977 (1980); *Rauscher*, in: Krüger/Rauscher, MünchKommZPO

Gericht bei der Durchführung der Einvernahme sein eigenes Prozessrecht an,[68] was insbesondere bei unterschiedlichen Gerichtssprachen[69] die Beteiligungsmöglichkeiten faktisch mindern kann.[70] Von nicht zu unterschätzender Bedeutung ist schließlich, dass das ersuchte Gericht bei Erledigung des Ersuchens auch *Zwangsmaßnahmen* anzuwenden hat, sofern dies nach dem Recht dieses Mitgliedstaats für die Erledigung eines zum gleichen Zweck gestellten Ersuchens inländischer Behörden vorgesehen ist (Art. 15 EuBVO).[71]

*c) Videoeinvernahme durch das ersuchende Gericht („passive Rechtshilfe")*

Bestimmungen über die unmittelbare Beweisaufnahme durch das ersuchende Gericht finden sich in den Art. 19 f. EuBVO; der mit der Revision geschaffene Art. 20 EuBVO sieht Sonderregeln für die unmittelbare Beweisaufnahme per Videokonferenz oder mittels anderer Fernkommunikationstechnologie vor.[72] Fraglich ist in diesem Zusammenhang insbesondere, ob durch diese Bestimmung nunmehr jegliche Videovernehmung einer Person im Ausland in das Regime der passiven Rechtshilfe kanalisiert wird[73] oder ob eine solche Vernehmung (auf freiwilliger Basis der einvernommenen Person) grundsätzlich auch ohne Einbeziehung der ausländischen Gerichte zulässig ist und Art. 20 EuBVO nur dann zur Anwendung zu bringen ist, wenn auf Videokonferenzanlagen der ausländischen Justizbehörden zurückgegriffen werden soll.[74] Aus den Entscheidungen des EuGH C-332/11 *ProRail* und C-188/22 *VP* kann wohl zuverlässig abgeleitet werden, dass der EuBVO eine zwingende Inanspruchnahme der passiven Rechtshilfeinstrumente nicht entnommen werden kann,[75]

---

III, 6. Aufl., 2022, Art. 11 EG-BewVO Rn. 1 ff. und Art. 12 EG-BewVO Rn. 1 ff.; *Sengstschmied*, in: Mayr, Handbuch, 2. Aufl., 2023, Rn. 15.165 ff., 15.171 ff.

[68] *Mosser*, in: Fasching/Konecny, Kommentar V/3, 3. Aufl., 2023, Art. 12 EuBVO 2020 Rn. 11; *Rauscher*, in: Krüger/Rauscher, MünchKommZPO III, 6. Aufl., 2022, Art. 10 EG-BewVO Rn. 5.

[69] Vgl. *Mosser*, in: Fasching/Konecny, Kommentar V/3, 3. Aufl., 2023, Art. 12 EuBVO 2020 Rn. 13; *Rauscher*, in: Krüger/Rauscher, MünchKommZPO III, 6. Aufl., 2022, Art. 10 EG-BewVO Rn. 5.

[70] Vgl. auch *Kohake*, DRiZ 2021, 378 (381).

[71] *Mosser*, in: Fasching/Konecny, Kommentar V/3, 3. Aufl., 2023, Art. 15 EuBVO 2020 Rn. 1 ff.; *Rauscher*, in: Krüger/Rauscher, MünchKommZPO III, 6. Aufl., 2022, Art. 13 EG-BewVO Rn. 1 ff.; *Sengstschmied*, in: Mayr, Handbuch, 2. Aufl., 2023, Rn. 15.180 ff.

[72] *Fucik*, in: Fasching/Konecny, Kommentar V/3, 3. Aufl., 2023, Art. 20 EuBVO 2020 Rn. 1; *Rauscher*, in: Krüger/Rauscher, MünchKommZPO III, 6. Aufl., 2022, Art. 17 EG-BewVO Rn. 30; *Sengstschmied*, in: Mayr, Handbuch, 2. Aufl., 2023, Rn. 15.218.

[73] So etwa *Knöfel*, Die Neufassung der Europäischen Beweisaufnahmeverordnung (EuBewVO), RIW 2021, 247 (250); *Lafontaine*, Die Beweisaufnahme über den EU-Auslandssachverhalt, DAR 2020, 541 (543); *Stadler*, in: Musielak/Voit (Hrsg.), ZPO. Zivilprozessordnung, 21. Aufl., 2024, § 1072 ZPO Rn. 3.

[74] So etwa *Garber*, in: Geimer/Schütze (Hrsg.), Europäisches Zivilverfahrensrecht. Kommentar, 4. Aufl., 2020, Art. 17 EuGFVO Rn. 2; *Oberhammer/Scholz-Berger*, ecolex 2022, 285 (289); *Rauscher*, in: Krüger/Rauscher, MünchKommZPO III, 6. Aufl., 2022, Art. 17 EG-BewVO Rn. 30; *Sengstschmied*, in: Mayr, Handbuch, 2. Aufl., 2023, Rn. 15.219.

[75] EuGH, Urt. v. 21.2.2013 – Rs. C-332/11 (ProRail) – Rn. 38 ff.; EuGH, Beschl. v. 8.9.2022 – Rs. C-188/22 (VP); so auch *Domej*, in: Stein/Jonas (Hrsg.), Kommentar zur Zivilprozessordnung:

wenngleich dies im Schrifttum teils auch anders gesehen wird.[76] Ob eine solche Inanspruchnahme *in concreto* notwendig ist, hängt vielmehr (gewissermaßen: subsidiär) davon ab, ob man in der freiwilligen Videoeinvernahme einer im Ausland befindlichen Person einen Eingriff in die territoriale Hoheitsgewalt dieses Staats erblicken will. Dies ist sowohl im österreichischen[77] als auch im deutschen[78] Schrifttum umstritten; in der Schweiz wird das Vorliegen eines Eingriffs – freilich nicht im Zusammenhang mit der EuBVO – hingegen bejaht.[79]

Ein Antrag gem. Art. 19 EuBVO ist aber jedenfalls erforderlich, wenn die ausländischen Gerichte in die Beweisaufnahme involviert werden sollen. Im Bereich der Videoeinvernahme kann das etwa dann notwendig sein, wenn seitens des ersuchenden Gerichts der Wunsch oder die Notwendigkeit besteht, die Videokonferenzinfrastruktur der ausländischen Gerichte in Anspruch zu nehmen.[80] Ein Vorgehen nach den Bestimmungen über die passive Rechtshilfe hat (verglichen mit der aktiven Rechtshilfe nach Art. 12 ff. EuBVO) den entscheidenden Vorteil, dass das ersuchende Gericht sein eigenes Verfahrensrecht anwenden[81] und damit bei der Einvernahme sich auch seiner eigenen Gerichtssprache bedienen kann.[82] Allerdings ist (darin liegt die „Kehrseite" der Medaille) eine unmittelbare Beweisaufnahme gem. Art. 19

---

ZPO XI, 23. Aufl., 2021, Art. 17 EuBVO Rn. 36 f.; *Oberhammer/Scholz-Berger*, ecolex 2022, 285 (289).

[76] Vgl. etwa *Lafontaine*, DAR 2020, 541 (550); *Zwettler*, Keine Videoeinvernahme von in der Schweiz aufhältigen Zeugen, Zak 2022, 227 (229).

[77] Ein Eingriff wird etwa *verneint* von *Oberhammer/Scholz-Berger*, ecolex 2022, 285 (289); *Sengstschmid*, in: Fasching/Konecny, Kommentar I, 3. Aufl., 2013, § 38 JN Rn. 51; *Sengstschmied*, in: Mayr, Handbuch, 2. Aufl., 2023, Rn. 15.57; vorsichtiger *Melzer*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 132a ZPO Rn. 24 (es seien „grundsätzlich völkerrechtliche territoriale Souveränitätsaspekte zu beachten"); *bejaht* hingegen von *Exenberger/Karl*, Grenzüberschreitende Aufnahme von Personalbeweisen Post-Brexit, ecolex 2021, 736 (738) und *Fucik*, in: Fasching/Konecny, Kommentar V/3, 3. Aufl., 2023, Art. 20 EuBVO 2020 Rn. 5.

[78] Ein Eingriff wird etwa *verneint* von VG Freiburg, Beschl. v. 11.3.2022 – 10 K 4411/19 RIW 2022, 476 (allerdings in Bezug auf eine Videoverhandlung); *Berger*, in: Stein/Jonas, Kommentar V, 23. Aufl., 2015, § 363 ZPO Rn. 14; *Geimer*, Internationales Zivilprozessrecht, 9. Aufl., 2024, Rn. 2385a; *Knöfel*, Videokonferenztechnologie im grenzüberschreitenden Zivilprozess, RIW 2022/7, Umschlagteil I; *Nagel/Gottwald*, Internationales Zivilprozessrecht, 8. Aufl., 2020, Rn. 9.140; *bejaht* hingegen von *Fritsche*, in: Krüger/Rauscher, MünchKommZPO I, 6. Aufl., 2020, § 128a ZPO Rn. 3; *Lafontaine*, DAR 2020, 541 (543); *Schultzky*, Videokonferenzen im Zivilprozess, NJW 2003, 313 (314); *Stadler*, in: Musielak/Voit, ZPO, 21. Aufl., 2024, § 128a ZPO Rn. 2a, 8; *Windau*, Die Verhandlung im Wege der Bild- und Tonübertragung, NJW 2020, 2753 (2754).

[79] *Schweizerisches Bundesamt für Justiz*, Die internationale Rechtshilfe in Zivilsachen. Wegleitung, 3. Aufl., 2003 (Stand Juli 2024), 35, abrufbar unter https://www.rhf.admin.ch/rhf/de/home/zivilrecht/wegleitungen.html (Abrufdatum: 9.1.2025); *Gauthey/Markus*, Zivile Rechtshilfe und Art. 271 Strafgesetzbuch, ZSR 2015, 359 (388 f., 394); vgl. auch *Zwettler*, Zak 2022, 227 (228).

[80] *Sengstschmied*, in: Mayr, Handbuch, 2. Aufl., 2023, Rn. 15.80, 15.220.

[81] *Fucik*, in: Fasching/Konecny, Kommentar V/3, 3. Aufl., 2023, Art. 19 EuBVO 2020 Rn. 16; *Rauscher*, in: Krüger/Rauscher, MünchKommZPO III, 6. Aufl., 2022, Art. 17 EG-BewVO Rn. 18; *Sengstschmied*, in: Mayr, Handbuch, 2. Aufl., 2023, Rn. 15.208.

[82] *Fucik*, in: Fasching/Konecny, Kommentar V/3, 3. Aufl., 2023, Art. 19 EuBVO 2020 Rn. 16; *Rauscher*, in: Krüger/Rauscher, MünchKommZPO III, 6. Aufl., 2022, Art. 17 EG-BewVO Rn. 20; *Sengstschmied*, in: Mayr, Handbuch, 2. Aufl., 2023, Rn. 15.208.

Abs. 2 EuBVO nur statthaft, wenn sie freiwillig und ohne Einsatz von Zwangsmaßnahmen durchgeführt werden kann.[83] Interessant ist im Zusammenhang mit der passiven Rechtshilfe die mit der Revision der EuBVO geschaffene (technisch allerdings etwas umständlich geratene) Zustimmungsfiktion des Art. 19 Abs. 5 EuBVO, die bei Säumnis des ersuchten Gerichts dazu führt, dass von einer Stattgabe des Ersuchens ausgegangen wird.[84] Für die Videoeinvernahme ist dies gleichsam in aller Regel ohne Bedeutung, wenn man davon ausgeht, dass ein passives Rechtshilfeersuchen überhaupt nur bei gewünschter Involvierung des ersuchten Gerichts zu stellen ist (weil in diesem Fall ja tatsächlich ein Handeln des Gerichts begehrt wird).

Soweit eine unmittelbare Einvernahme durch ein österreichisches Gericht per Videokonferenztechnologie erfolgen soll, müssen nach nationalem Recht in jedem Fall die Voraussetzungen des § 277 öZPO (und damit mittelbar des § 328 Abs. 1, § 352 Abs. 1 bzw. § 375 Abs. 2 öZPO) erfüllt sein. Insofern sind die Anwendungsvoraussetzungen für die grenzüberschreitende Videoeinvernahme bei aktiver und passiver Rechtshilfe auf nationaler Ebene im Wesentlichen ident.

## III. Videoverhandlung

### *1. Allgemeines*

In einem zweiten Schritt soll die im österreichischen Rechtsbestand noch relativ junge Möglichkeit der Videoverhandlung dargestellt werden. Katalysator hierfür war (wie in vielen anderen Bereichen[85]) die COVID-19-Pandemie, die eine schnelle Anpassung des Justizsystems an die faktischen Gegebenheiten erforderte.[86] Teile der in diesem Zug zunächst nur temporär geltenden Bestimmungen wurden mit der ZVN 2023 in den neu geschaffenen § 132a öZPO gegossen und damit in den permanenten Rechtsbestand überführt.[87]

---

[83] *Fucik*, in: Fasching/Konecny, Kommentar V/3, 3. Aufl., 2023, Art. 19 EuBVO 2020 Rn. 15; *Rauscher*, in: Krüger/Rauscher, MünchKommZPO III, 6. Aufl., 2022, Art. 17 EG-BewVO Rn. 21; *Sengstschmied*, in: Mayr, Handbuch, 2. Aufl., 2023, Rn. 15.211; kritisch dazu etwa *Knöfel*, RIW 2021, 247 (252 ff.).

[84] Siehe etwa *Peer/Scheuer*, Neue europäische Instrumente zur grenzüberschreitenden Zustellung und Beweisaufnahme, Zak 2021, 27 (29).

[85] Vgl. beispielhaft etwa *Angermair/Artner/Brandstetter/Kessler/Kulmer/Pimmer/Schöller/Zahradnik*, COVID-19-Gesetze: Ausgewählte für Unternehmen relevante Regelungen. Von Arbeitsrecht bis Zivilprozess, NZ 2020, 121; *Bauer/Brunner/Scharl*, Digitale soziale Sicherung in Europa - ein wichtiger Schritt in die Zukunft, SozSi 2022, 68; *Vinzenz*, Ein schwarzer Tag im Homeoffice, DRdA 2023, 492; *Winkler*, „Rien ne vas plus" für den klassischen Anwalt? AnwBl 2021, 144.

[86] Siehe insbesondere *Koller*, Krise als Motor der Rechtsentwicklung im Zivilprozess- und Insolvenzrecht, JBl 2020, 539 (539 ff.); vgl. auch *Ent*, RZ 2023, 284 (284 ff.); *Fink*, in: Fink/Otti/Sommer, Zukunft, 1 (15 ff.); *Oberhammer/Scholz-Berger*, ecolex 2022, 285 (285); *Scholz-Berger/Schumann*, ecolex 2020, 469 (469 ff.); *Sengstschmid*, in: FS für Andreas Konecny, 553 (555).

[87] *Ent*, RZ 2023, 284 (285 f.); *Melzer*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 132a ZPO Rn. 1; *Spitzer/Wilfinger*, ZVN 2023: Videoverhandlung im Zivilprozess, ÖJZ 2023, 606 (606).

### *2. Nationaler Rechtsrahmen: § 132a öZPO*

#### *a) Ausgangslage und Gesetzgebungsprozess*

Während manche andere Rechtsordnungen auf geradezu „altehrwürdige" Bestimmungen zur digitalen Durchführung eines Zivilverfahrens verweisen können (der deutsche § 128a dZPO über die „Videoverhandlung" wurde etwa bereits im Jahr 2002 geschaffen[88]), waren dem österreichischen Zivilverfahrensrecht – von der in § 277 öZPO normierten Möglichkeit der digitalen Beweisaufnahme sowie dem praktisch kaum bedeutsamen Art. 8 EuBagatellVO[89] (dazu noch in Abschnitt III.3.) abgesehen – solche Instrumente bis in die jüngste Vergangenheit noch fremd. Pandemiebedingt mussten freilich schnell pragmatische Lösungen gefunden werden: § 3 des 1. COVID-19 JuBG ermöglichte es, (in den meisten Verfahrensarten: mit Einverständnis der Parteien) sowohl mündliche Verhandlungen als auch Beweisaufnahmen unter Verwendung geeigneter technischer Kommunikationsmittel zur Wort- und Bildübertragung durchzuführen, und zwar unabhängig vom Vorliegen der Voraussetzungen des § 277 öZPO.[90] Die Geltung dieser zunächst bloß befristeten „Notfalllösung"[91] wurde aufgrund faktischer Notwendigkeiten mehrfach (letztlich bis zum 30.6.2023) verlängert;[92] gleichzeitig verfestigten sich die Bestrebungen, Bestimmungen über eine Videoverhandlung auch ins Dauerrecht aufzunehmen.[93] Ein entsprechender erster Entwurf zu einer ZVN 2021[94] wurde seitens der Praxis allerdings noch überwiegend kritisch gesehen: Der Österreichische Rechtsanwaltskammertag ortete etwa eine „drohende Verletzung des Unmittelbarkeitsgrundsatzes"[95], die Vereinigung der österreichischen Richterinnen und Richter befürchtete unter anderem unerlaubte Aufzeichnungen der Verhandlungen und trat für eine Neuevaluierung der vorgesehenen Bestimmung ein.[96] Die geplante Gesetzesnovelle wurde (in diesem Punkt) daher vorübergehend auf Eis gelegt und eine breit angelegte Arbeits-

---

[88] *Fritsche*, in: Krüger/Rauscher, MünchKommZPO I, 6. Aufl., 2020, § 128a ZPO Rn. 1; *Fuhrmann/Merks*, Videoverhandlung im Zivilverfahren, ZRP 2023, 66 (66); *Stadler*, in: Musielak/Voit, ZPO, 21. Aufl., 2024, § 128a ZPO Rn. 1.

[89] *Koller*, JBl 2020, 539 (546 [Fn. 92]); *Sengstschmid*, in: FS für Andreas Konecny, 553 (554).

[90] Dazu etwa *Garber/Neumayr*, in: Resch (Hrsg.), Corona-Handbuch, Vers. 1.06, 2021, Kapitel 13 Rn. 54 ff.; *Leupold*, Öffentlichkeit im Zivilprozess. Verfahrensgrundsätze und Rechtsentwicklung im Lichte der Krise, JRP 2021, 339 (347); *Scholz-Berger/Schumann*, ecolex 2020, 469 (469 ff.); *Sengstschmid*, in: FS für Andreas Konecny, 553 (556).

[91] *Spitzer/Wilfinger*, ÖJZ 2023, 606 (606).

[92] *Ent*, RZ 2023, 284 (285); *Spitzer*, in: FS für Elisabeth Lovrek, 725 (733); *Spitzer/Wilfinger*, ÖJZ 2023, 606 (606); vgl. auch *Sengstschmid*, in: FS für Andreas Konecny, 553 (555).

[93] *Ent*, RZ 2023, 284 (285); *Leupold*, JRP 2021, 339 (352); *Sengstschmid*, in: FS für Andreas Konecny, 553 (554); *Spitzer*, in: FS für Elisabeth Lovrek, 725 (733 ff.).

[94] ME ZVN 2021, 138/ME 27. GP; zu diesem etwa *Fink*, in: Fink/Otti/Sommer, Zukunft, 1 (17 ff.); *Leupold*, JRP 2021, 339 (352 f.).

[95] Österreichischer Rechtsanwaltskammertag, Stellungnahme zum ME einer Zivilverfahrens-Novelle 2021, 30/SN-138/ME, 6.

[96] *Vereinigung der österreichischen Richterinnen und Richter*, Stellungnahme zum ME einer Zivilverfahrens-Novelle 2021, 43/SN-138/ME, 4 f.

gruppe unter stärkerer Einbindung von Wissenschaft und Praxis eingesetzt.[97] Mit der ZVN 2023 wurde der Zivilprozessordnung schließlich die Bestimmung des § 132a öZPO hinzugefügt, in deren Rahmen Videoverhandlungen nunmehr unter gewissen Voraussetzungen möglich sind; auch das AußStrG (§ 18 Abs. 2 und 3), die EO (§ 59a) und die IO (§ 254 Abs. 3a) wurden in diesem Zusammenhang angepasst.[98]

*b) Anwendungsvoraussetzungen*

Gem. § 132a Abs. 1 S. 2 öZPO kann das Gericht eine Tagsatzung zur mündlichen Verhandlung ohne persönliche Anwesenheit von Parteien, ihren Vertretern und sonst der Verhandlung beizuziehenden Personen *unter Verwendung geeigneter technischer Kommunikationsmittel zur Wort- und Bildübertragung durchführen* sowie auf diese Weise auch ohne Vorliegen der Voraussetzungen des § 277 öZPO *Gutachten* von gerichtlich bestellten Sachverständigen *mündlich erstatten lassen oder erörtern* und die *Parteien und informierte Personen* (§ 258 Abs. 2 öZPO) *in der vorbereitenden Tagsatzung vernehmen*. Voraussetzung dafür ist gem. S. 2 *leg. cit*., dass diese Vorgangsweise unter dem Gesichtspunkt der Verfahrensökonomie tunlich ist, die technischen Voraussetzungen vorhanden sind, um die Tagsatzung verfahrenskonform abzuhalten, und nicht eine Partei innerhalb einer vom Gericht festgesetzten angemessenen Frist dem angekündigten Vorgehen widerspricht oder die ausdrückliche Zustimmung der Parteien dazu vorliegt.

*Tunlichkeit* nimmt die herrschende Auffassung etwa dann an, wenn durch die Videoverhandlung eine Vertagung vermieden oder die Verfahrenskosten gesenkt werden könnten, weil der Anreiseaufwand zum Gericht geringer ist.[99] Der Gesetzgeber selbst hat hierbei insbesondere an kurze Tagsatzungen mit wenig Interaktion zwischen Gericht und Parteien gedacht[100] und wollte mit dieser Voraussetzung zudem den Ausnahmecharakter der Videoverhandlung betonen.[101]

Das *Vorliegen der technischen Voraussetzungen zur verfahrenskonformen Abhaltung der Tagsatzung* inkludiert nach den Gesetzesmaterialien nicht nur die entsprechende technische Ausstattung des Entscheidungsorgans selbst, sondern auch, dass das Gericht über die technischen Anlagen verfügen muss, die es bei einer öffentlichen mündlichen Verhandlung der (Volks-)Öffentlichkeit ermöglichen, dem Verfahrensgeschehen optisch und akustisch zu folgen.[102] Die Volksöffentlichkeit soll

---

[97] *Ent*, RZ 2023, 284 (285 f.); *Sengstschmid*, in: FS für Andreas Konecny, 553 (555).

[98] Zum AußStrG etwa ausführlich *Barth*, Die „Videoverhandlung" in familienrechtlichen Verfahren - eine Kurzübersicht, iFamZ 2023, 260 (260); zu IO und EO etwa *Eriksson*, Die Zivilverfahrens-Novelle 2023, ZIK 2023, 164 (164 ff.).

[99] *Ent*, RZ 2023, 284 (286); *Hotter*, ZVN 2023: Die Übernahme der Videoverhandlung ins Dauerrecht, ecolex 2023, 763 (764).

[100] ErläutRV 2093 BlgNR 27. GP 3; *Ent*, RZ 2023, 284 (286).

[101] ErläutRV 2093 BlgNR 27. GP 4; *Ent*, RZ 2023, 284 (286); *Hotter*, ecolex 2023, 763 (763); *Melzer*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 132a ZPO Rn. 17.

[102] ErläutRV 2093 BlgNR 27. GP 4; dazu auch *Ent*, RZ 2023, 284 (285 f.).

nach den Materialien dadurch gewahrt werden, dass sich zumindest der Richter während der gesamten Verhandlung im Gerichtssaal aufhalten muss und die Zuhörer weiterhin dort dem Prozessgeschehen (optisch und akustisch[103]) folgen können.[104] Teils scheint es hier in der Praxis derzeit allerdings (mangels flächendeckender Ausstattung der Verhandlungssäle mit großen Bildschirmen, auf denen auch Zuseher das Geschehen wahrnehmen können) noch gewisse Probleme zu geben.[105] Die „verfahrenskonforme Abhaltung der Tagsatzung" umfasst auch die Beachtung datenschutzrechtlicher Sicherheitsstandards sowie allenfalls die Gewährleistung einer barrierefreien Verfahrensteilnahme für Menschen mit Behinderung.[106] In diesem Zusammenhang wurde mit der ZVN 2023 auch die mit „Datensicherheit bei mündlichen Verhandlungen im Wege von Bild- und Tonübertragungen" übertitelte Bestimmung des § 85b GOG geschaffen:[107] Demnach sind bei einer Videoverhandlung nur die vom Bundesministerium für Justiz zur Verfügung gestellten Systeme heranzuziehen (Abs. 1 Z. 1), Bild und Ton sind verschlüsselt zu übermitteln (Abs. 1 Z. 2), der Zugang zu den Bild- und Tonübertragungssystemen ist auf die nach den Verfahrensgesetzen zuzulassenden Personen zu beschränken sowie entsprechend dem Stand der Technik (insbesondere durch Absicherung der Einwahl mittels Passworts[108]) abzusichern (Abs. 1 Z. 3) und die Videokonferenz darf nur für die einmalige Verwendung angelegt werden (Abs. 1 Z. 4). Von diesen Vorgaben kann gem. § 85b Abs. 3 GOG nur bei Gefahr in Verzug oder dann abgewichen werden, wenn die Bild- und Tonübertragung auf andere Weise nicht durchführbar ist. Voraussetzung ist es zudem, dass die Bild- und Tonübertragung aufgrund der Umstände des Einzelfalls unbedingt erforderlich ist und durch sonstige technische und organisatorische Maßnahmen angemessene Datensicherheit gewährleistet werden kann. Bei Überprüfung der technischen Voraussetzungen hat das Gericht nicht nur seine eigenen Möglichkeiten, sondern auch jene der zu involvierenden Personen zu beachten,[109] zumal der Anwendungsbereich des § 132a öZPO – abgesehen von der Ausnahme für Eheverfahren in § 460 Z. 1a öZPO – nicht von einer anwaltlichen Vertretung der digital teilnehmenden Personen abhängt.[110]

Letzte Voraussetzung für die Durchführung einer Videoverhandlung ist es schließlich, dass entweder die *ausdrückliche Zustimmung der Parteien* dazu vorliegt oder *nicht eine Partei innerhalb einer vom Gericht festgesetzten angemessenen Frist dem angekündigten Vorgehen widerspricht.* Daraus ergibt sich, dass das Gericht den Parteien rechtzeitig anzukündigen hat, dass eine bevorstehende Tagsatzung in Form

---

[103] *Melzer*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 132a ZPO Rn. 18.
[104] ErläutRV 2093 BlgNR 27. GP 2 f.
[105] *Ent*, RZ 2023, 284 (288).
[106] ErläutRV 2093 BlgNR 27. GP 4.
[107] Dazu *Ent*, RZ 2023, 284 (287).
[108] *Ent*, RZ 2023, 284 (287).
[109] *Spitzer/Wilfinger*, ÖJZ 2023, 606 (607).
[110] *Spitzer/Wilfinger*, ÖJZ 2023, 606 (607).

einer Videoverhandlung durchgeführt werden soll.[111] Nicht zuletzt aufgrund der kritischen Äußerungen im Begutachtungsverfahren zur ZVN 2021 wollte der Gesetzgeber durch das Erfordernis der Zustimmung (bzw. des nicht rechtzeitigen Widerspruchs) sicherstellen, dass niemand gegen seinen Willen dazu verhalten wird, diese in nicht unerheblichen Aspekten andersartige Verhandlungssituation hinnehmen zu müssen.[112] Konsequenterweise bedarf der Widerspruch einer Partei daher auch keiner Begründung,[113] was im Schrifttum teils kritisch gesehen wird.[114] Ein verspäteter Widerspruch ist meines Erachtens grundsätzlich ebenso unbeachtlich (zumal es andernfalls der Normierung einer Fristsetzungsmöglichkeit gar nicht bedurft hätte) wie der Widerruf einer einmal erteilten Zustimmung.[115] Wenn freilich im Nachhinein besondere, eine Partei an der digitalen Verfahrensteilnahme hindernde Umstände auftreten (die etwa eine Vertagung oder gar eine Wiedereinsetzung in den vorigen Stand rechtfertigen würden), dann wird das Gericht dennoch eine (zumindest teilweise; vgl. dazu gleich) analoge Verhandlung durchzuführen haben;[116] dies ergibt sich aus einem Größenschluss zu § 134 Z. 1 öZPO (dazu noch unten in Abschnitt III.2.c).

*c) Rechtsfolge: Digitale Verhandlung und teilweise digitale Beweisaufnahmen*

Sind die Anwendungsvoraussetzungen gegeben, so erfolgt die Anberaumung einer Videoverhandlung auf entsprechende gerichtliche Anordnung;[117] dies liegt im Ermessen des Gerichts.[118] Den Parteien kommt kein entsprechendes Antragsrecht zu; sie können die Durchführung einer Videoverhandlung lediglich anregen (§ 132a Abs. 1 letzter S. öZPO).[119] Das Entscheidungsorgan hat bei der Durchführung einer Videoverhandlung im Gerichtsgebäude anwesend zu sein (das ergibt sich aus § 132 Abs. 1 öZPO);[120] dadurch soll nicht zuletzt die Volksöffentlichkeit des Verfahrens

---

[111] *Melzer*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 132a ZPO Rn. 7.

[112] ErläutRV 2093 BlgNR 27. GP 3; vgl. auch *Melzer*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 132a ZPO Rn. 12.

[113] ErläutRV 2093 BlgNR 27. GP 3; *Melzer*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 132a ZPO Rn. 9.

[114] *Hotter*, ecolex 2023, 763 (763 f.).

[115] So wohl auch *Spitzer/Wilfinger*, ÖJZ 2023, 606 (607); etwas liberaler *Ent*, RZ 2023, 284 (291 f.).

[116] *Spitzer/Wilfinger* (ÖJZ 2023, 606 [607]) sprechen – im Ergebnis ident – davon, dass in solchen Fällen auch nachträglich eine Widerspruchsmöglichkeit einzuräumen sei.

[117] *Barth*, iFamZ 2023, 260 (261); *Melzer*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 132a ZPO Rn. 3.

[118] *Melzer*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 132a ZPO Rn. 4; *Spitzer/Wilfinger*, ÖJZ 2023, 606 (607).

[119] *Melzer*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 132a ZPO Rn. 3; *Spitzer/Wilfinger*, ÖJZ 2023, 606 (607).

[120] ErläutRV 2093 BlgNR 27. GP 2; *Barth*, iFamZ 2023, 260 (261); *Hotter*, ecolex 2023, 763 (764); *Melzer*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 132a ZPO Rn. 5; dies (trotz insoweit ausdrücklicher Gesetzesmaterialien) anzweifelnd *Ent*, RZ 2024, 56 (62 f.).

sichergestellt werden.[121] Eine *„hybride" Verhandlung* (wie sie etwa § 128a Abs. 4 dZPO nach einem Einspruch explizit vorsieht) ist in § 132a öZPO zwar nicht ausdrücklich erlaubt, aus den Gesetzesmaterialien erschließt sich aber eindeutig, dass der Gesetzgeber auch eine solche Vorgangsweise für zulässig erachtet.[122] Derzeit scheinen die Gerichte allerdings gerade für hybride Videoverhandlungen noch nicht flächendeckend technisch gerüstet zu sein.[123]

Der tatsächliche Anwendungsbereich des § 132a öZPO ist bei genauerer Betrachtung weniger groß, als dies auf den ersten Blick den Anschein haben mag: Zunächst wird in Abs. 1 zwar (eher allgemein) angeordnet, dass das Gericht „eine Tagsatzung zur mündlichen Verhandlung ohne Anwesenheit von Parteien, ihren Vertretern oder sonst der Verhandlung beizuziehenden Personen unter Verwendung geeigneter technischer Kommunikationsmittel zur Wort- und Bildübertragung durchführen" kann. Bei einer solcherart digital durchgeführten Tagsatzung können sowohl das Gericht als auch die Parteien grundsätzlich alle Verfahrenshandlungen vornehmen.[124] Allerdings ergibt sich aus dem zweiten Teil dieses ersten Satzes (arg.: „sowie auf diese Weise auch ohne Vorliegen der Voraussetzungen des § 277 Gutachten von gerichtlich bestellten Sachverständigen mündlich erstatten lassen oder erörtern und die Parteien und informierte Personen [§ 258 Abs. 2] in der vorbereitenden Tagsatzung vernehmen"), dass *Beweisaufnahmen* weiterhin grundsätzlich nur unter den Voraussetzungen des § 277 öZPO per Videokonferenztechnologie durchgeführt werden dürfen.[125] Anderes gilt *expressis verbis* für die Erstattung und Erörterung von Sachverständigengutachten im Allgemeinen sowie für die Einvernahme der Parteien und informierter Personen (letztere nach dem Willen des Gesetzgebers offenbar als Zeugen[126]) in der vorbereitenden Tagsatzung.[127] Die Einschränkung der digitalen Parteienvernehmung auf die vorbereitende Tagsatzung ist sachlich nicht ganz konsequent,[128] lässt sich aber mit dem Wunsch des Gesetzgebers erklären, die (in aller Regel rasch abzuhandelnde) vorbereitende Tagsatzung ganz generell digital durchführen zu können.[129]

---

[121] ErläutRV 2093 BlgNR 27. GP 2 f.; *Ent*, RZ 2024, 56 (63); *Koller*, JBl 2020, 539 (542 f.); *Melzer*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 132a ZPO Rn. 5; kritisch (allerdings zum Entwurf nach der ZVN 2021) *Wimmer*, Der Schutz der Persönlichkeit im digitalisierten Verwaltungsverfahren. Zugleich ein Versuch der Kontextualisierung, JRP 2022, 483.

[122] ErläutRV 2093 BlgNR 27. GP 2; *Barth*, iFamZ 2023, 260 (261); *Ent*, RZ 2024, 56 (63 f.); *Melzer*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 132a ZPO Rn. 4; *Spitzer/Wilfinger*, ÖJZ 2023, 606 (607).

[123] *Ent*, RZ 2024, 56 (63).

[124] *Melzer*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 132a ZPO Rn. 2.

[125] *Ent*, RZ 2024, 56 (56); *Melzer*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 132a ZPO Rn. 14; *Oberhammer/Scholz-Berger*, ecolex 2022, 285 (285 f.); *Spitzer*, in: Spitzer/Wilfinger, Beweisrecht, 2020, § 277 ZPO Rn. 5 ff.; *Spitzer/Wilfinger*, ÖJZ 2023, 606 (607).

[126] ErläutRV 2093 BlgNR 27. GP 2; ebenso *Ent*, RZ 2024, 56 (58); *Spitzer/Wilfinger*, ÖJZ 2023, 606 (608).

[127] *Melzer*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 132a ZPO Rn. 2.

[128] So schon *Ent*, RZ 2024, 56 (58); *Spitzer*, in: FS für Elisabeth Lovrek, 725 (739); *Spitzer/Wilfinger*, ÖJZ 2023, 606 (608).

[129] *Spitzer*, in: FS für Elisabeth Lovrek, 725 (739); *Spitzer/Wilfinger*, ÖJZ 2023, 606 (608).

Die Bestimmungen der § 277 und 132a öZPO können im Übrigen „nebeneinander" angewendet werden,[130] sodass etwa die Aufnahme eines Sachverständigenbeweises gem. § 132a öZPO, die Einvernahme von Zeugen hingegen nach § 277 i. V. m. § 328 Abs. 1 öZPO im Rahmen einer Videoverhandlung erfolgen können.

Eine interessante Neuerung wurde – aufgrund von Bedenken hinsichtlich der reibungslosen Funktionalität der Videoverhandlung[131] – auch der Liste an Gründen hinzugefügt, aufgrund derer die Erstreckung einer Tagsatzung statthaft ist: Gem. § 134 Z. 1 zweiter Fall öZPO kann eine solche für den Fall einer technischen Störung der Wort- und Bildübertragung bei einer nach § 132a öZPO anberaumten Tagsatzung auch dann angeordnet werden, wenn eine Partei ohne die Erstreckung einen *prozessualen Nachteil* erleiden würde. Das soll nach den Materialien etwa bereits dann der Fall sein, wenn „die Partei […] die Möglichkeit verliert, Vorbringen im Verfahren zu erstatten oder sich an einer Vernehmung oder Erörterung eines Sachverständigengutachtens zu beteiligen oder ihr Kostenersatzfolgen erwachsen."[132] Dass die Anwendungskriterien hier deutlich weniger streng als bei herkömmlichen Erstreckungen sind (arg.: „nicht wieder gut zu machenden Schaden"), begründet der Gesetzgeber damit, dass die mannigfaltigen Ursachen für technische Störungen bei Videokonferenzen mehrheitlich nicht von den Parteien kontrolliert oder verhindert werden könnten.[133] Für diese Fälle sei es notwendig, möglichst einfache und den prozessualen Aufwand gering haltende Lösungen zur Verfügung zu stellen, die allerdings auf der anderen Seite einem allfälligen Missbrauch ausreichend vorbeugen.[134] Seitens der Praxis wird allerdings darauf hingewiesen, dass es sehr wohl erhebliches Missbrauchspotential gebe, eine Erstreckung zu erzwingen, zumal für das Gericht kaum überprüfbar sei, wodurch etwa ein Verbindungsabbruch entstanden ist.[135] Im Schrifttum wird teils einer analogen Anwendung dieser Bestimmung auf Situationen das Wort geredet, in welchen zwar streng genommen keine „technische Störung" vorliegt, die Partei aber aus technischer Unkenntnis (etwa, weil das Mikrofon oder das richtige Audioausgabegerät nicht aktiviert werden konnte) trotz ernsthaften Bemühens nicht an der Verhandlung teilnehmen konnte.[136]

Wurden die Anwendungsvoraussetzungen für die Durchführung einer Videoverhandlung missachtet, so kann dies einen wesentlichen Verfahrensmangel gem. § 496 Abs. 1 Z. 2 öZPO darstellen.[137] Eine im Schrifttum teils angenommene Nichtigkeit

---

[130] *Ent*, RZ 2024, 56 (56); *Hotter*, ecolex 2023, 763 (763); *Melzer*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 132a ZPO Rn. 14.

[131] Vgl. ErläutRV 2093 BlgNR 27. GP 5.

[132] ErläutRV 2093 BlgNR 27. GP 5.

[133] ErläutRV 2093 BlgNR 27. GP 5.

[134] ErläutRV 2093 BlgNR 27. GP 5.

[135] *Ent*, RZ 2024, 56 (65); Österreichischer Rechtsanwaltskammertag, Stellungnahme zum ME einer Zivilverfahrens-Novelle 2023, 6, abrufbar unter https://www.oerak.at/uploads/tx_wxstellungnahmen/13_1_23_48_zpo_eo.pdf (Abrufdatum: 9.1.2025); vgl. auch *Koller*, JBl 2020, 539 (541).

[136] *Ent*, RZ 2024, 56 (65).

[137] *Ent*, Videoverhandlungen nach der ZVN 2023 (Teil 3), RZ 2024, 91 (93).

(etwa wegen Verletzung des rechtlichen Gehörs [§ 477 Abs. 1 Z. 4 öZPO][138] oder wegen Ausschlusses der Öffentlichkeit [§ 477 Abs. 1 Z. 7 öZPO][139]), wird – angesichts der insoweit sehr strengen Judikatur des OGH[140] – meines Erachtens nur in extremen Ausnahmefällen zu bejahen sein.

*d) Sonderbestimmungen zu Kostenverzeichnis und Vergleichsabschluss*

§ 132a Abs. 2 und 3 öZPO enthalten „Spezialbestimmungen" für Sonderprobleme, die sich daraus ergeben, dass die Parteien und Parteienvertreter nicht physisch im Gerichtssaal anwesend sind:[141] Abweichend zu § 54 Abs. 1 öZPO, wonach *Kostenverzeichnisse* (bei sonstigem Verlust des Kostenersatzanspruchs) dem Gericht vor Schluss der mündlichen Hauptverhandlung übergeben werden müssen,[142] normiert § 132a Abs. 2 öZPO, dass bei Durchführung einer Verhandlung als Videoverhandlung die Vorlage des Kostenverzeichnisses als rechtzeitig gilt, wenn es spätestens bis zum Ablauf des auf die mündliche Verhandlung folgenden Tages dem Gericht übermittelt wird. Die Frist für die Erhebung von Einwendungen durch den Gegner (§ 54 Abs. 1a öZPO) beginnt diesfalls mit der Zustellung des Kostenverzeichnisses durch das Gericht an diesen. Unvertretene Parteien können das Kostenverzeichnis in der Tagsatzung sogar mündlich zu Protokoll anbringen.

§ 132a Abs. 3 öZPO normiert demgegenüber Besonderheiten für den Abschluss eines *gerichtlichen Vergleichs* in einer Videoverhandlung: Mit der ZVN 2022 hat der Gesetzgeber in § 209 Abs. 3 öZPO klargestellt,[143] dass die Unterschrift der Parteien für die Wirksamkeit eines gerichtlichen Vergleichs erforderlich ist. Für einen Vergleichsabschluss während einer Videoverhandlung normiert nun § 132a Abs. 3 öZPO, dass § 209 Abs. 3 zweiter und dritter Satz nicht anzuwenden und damit in diesem Fall keine Unterschrift erforderlich ist.[144] Stattdessen hat das Gericht (gewissermaßen als Ersatz für die verfestigte Willensbekundung durch Unterschrift[145]) zunächst entweder den Text des Vergleichs den Parteien auf dem Bildschirm sichtbar zu machen oder den Vergleichstext deutlich vorzulesen beziehungsweise den auf einem Tonträger aufgenommenen Vergleichstext für alle deutlich hörbar abzuspie-

---

[138] *Ent*, RZ 2024, 91 (93 f.).

[139] *Ent*, RZ 2024, 91 (94).

[140] Zur Nichtigkeit wegen Verletzung des rechtlichen Gehörs siehe etwa OGH 26.9.1985, 6 Ob 643/84; 17.1.2019, 5 Ob 220/18s; RIS-Justiz RS0042202; zur Nichtigkeit wegen Ausschlusses der Volksöffentlichkeit siehe etwa OGH 10.5.1989, 9 ObA 120/89; RIS-Justiz RS0036693.

[141] ErläutRV 2093 BlgNR 27. GP 4; *Melzer*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 132a ZPO Rn. 21.

[142] *M. Bydlinski*, in: Fasching/Konecny, Kommentar II/1, 3. Aufl., 2014, § 54 ZPO Rn. 5; *Ziehensack*, Praxiskommentar Kostenrecht, 2020, Rn. 551.

[143] Dies war zuvor strittig; vgl. dazu *Anzenberger*, Der gerichtliche Vergleich, 2020, 397 ff.; *Gitschthaler*, in: Rechberger/Klicka, ZPO, 5. Aufl., 2019, §§ 204–206 ZPO Rn. 13; *Klicka*, in: Fasching/Konecny, Kommentar II/3, 3. Aufl., 2015, § 206 ZPO Rn. 26; *Trenker/Werner*, Der Gerichtliche Vergleich nach der ZVN 2022. Protokollierung und Gebühren, RZ 2023, 62 (64).

[144] *Barth*, iFamZ 2023, 260 (261).

[145] Vgl. *Melzer*, in: Kodek/Oberhammer, ZPO-ON, 2023, § 132a ZPO Rn. 23.

len. In weiterer Folge muss der Wille der nicht persönlich anwesenden Parteien, diesen gerichtlichen Vergleich abzuschließen, unter Bedachtnahme auf die technischen Gegebenheiten klar und deutlich zum Ausdruck kommen; dies gilt auch für den Abschluss eines prätorischen Vergleichs.

### *3. Videoverhandlungen in europäischen Zivilverfahren: Art. 8 EuBagatellVO*

Anders als bei der Beweisaufnahme (vgl. Abschnitt II.3.) kennt das Europäische Zivilverfahrensrecht (noch; vgl. aber Abschnitt III.4.) keine auf die Verfahrensordnungen der Mitgliedstaaten „durchschlagenden" Bestimmungen über die Durchführung von Videoverhandlungen. Lediglich das (genuin europäische[146]) Bagatellverfahren sah schon in seiner Stammfassung in Art. 8 EuBagatellVO die (damals allerdings noch eher rudimentär ausformulierte) Möglichkeit vor, eine mündliche Verhandlung „über Videokonferenz oder unter Zuhilfenahme anderer Mittel der Kommunikationstechnologie" abzuhalten. Die seit 14.7.2017 geltende[147] revidierte Fassung der EuBagatellVO regelt diesen Punkt nunmehr deutlich ausführlicher (dazu gleich). Allerdings sind Verfahren nach der EuBagatellVO gem. deren Art. 5 Abs. 1 *grundsätzlich schriftlich* durchzuführen; nur ausnahmsweise hat nach Art. 5 Abs. 1a EuBagatellVO eine mündliche Verhandlung stattzufinden.[148] Dazu kommt die vergleichsweise sehr geringe Praxisrelevanz der Verfahren nach der EuBagatellVO,[149] sodass die Rahmenbedingungen für die Durchführung einer Videoverhandlung an dieser Stelle *nur überblicksartig dargestellt* werden sollen.

Für den (ausnahmsweisen; vgl. Art. 5 Abs. 1a EuBagatellVO) Fall der Durchführung einer mündlichen Verhandlung normiert Art. 8 Abs. 1 UAbs. 1 EuBagatellVO, dass hierfür dem Gericht zur Verfügung stehende geeignete *Mittel der Fernkommunikation genutzt* werden, es sei denn, dass dies in Anbetracht der besonderen Umstände des Falls für den Ablauf eines fairen Verfahrens nicht angemessen wäre. Das *Einverständnis der Parteien* oder ihrer Vertreter ist (anders als nach dem ursprünglichen Entwurf der Kommission[150]) hierfür nicht erforderlich.[151] Die Zulässigkeit der

---

[146] Vgl. *Mayr*, in: Mayr, Handbuch, 2. Aufl., 2023, Rn. 12.11.

[147] *Mayr*, in: Mayr, Handbuch, 2. Aufl., 2023, Rn. 12.6.

[148] *Varga*, in: Rauscher (Hrsg.), Europäisches Zivilprozess- und Kollisionsrecht. EuZPR/EuIPR II/1, 5. Aufl., 2022, Art. 8 EG-BagatellVO Rn. 1.

[149] *Mayr*, Europäisches Zivilprozessrecht, 2. Aufl., 2020, Rn. VI/2; *Mayr*, in: Mayr, Handbuch, 2. Aufl., 2023, Rn. 12.10; vgl. auch *Scheuer*, in: Fasching/Konecny, Kommentar V/3, 3. Aufl., 2023, Art. 1 EuBagatellVO Rn. 3.

[150] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Einführung eines europäischen Verfahrens für geringfügige Forderungen, Brüssel, den 15.3.2005, KOM(2005) 87 endg., 14, abrufbar unter https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0087:FIN:DE:PDF (Abrufdatum: 9.1.2025).

[151] *Hau*, in: Krüger/Rauscher, MünchKommZPO III, 6. Aufl., 2022, Art. 8 EG-BagatellVO Rn. 2; *Mayr*, in: Mayr, Handbuch, 2. Aufl., 2023, Rn. 12.74; *Mosser*, in: Geroldinger/Neumayr (Hrsg.), IZVR. Praxiskommentar Internationales Zivilverfahrensrecht II, 2021, Art. 8 EuBagVO Rn. 1; *Scheuer*, in: Fasching/Konecny, Kommentar V/3, 3. Aufl., 2023, Art. 8 EuBagatellVO Rn. 1; *Varga*, in: Rauscher, EuZPR/EuIPR II/1, 5. Aufl., 2022, Art. 8 EG-BagatellVO Rn. 2.

Durchführung einer Verhandlung im Weg der Videokonferenz nach Art. 8 EuBagatellVO hängt nach herrschender Auffassung zwar nicht davon ab, dass diese nach der *lex fori* des Prozessgerichts vorgesehen ist,[152] faktisch werden aber (aufgrund der Notwendigkeiten des Art. 6 EMRK bzw. Art. 47 GRC sowie aus Gründen der Datensicherheit) aber wohl nur „geeignete Mittel" zur Verfügung stehen, wenn auch das einschlägige nationale Verfahrensrecht ebenfalls eine Videoverhandlung kennt. Eine mitgliedstaatliche Verpflichtung zur Einrichtung solcher Mittel der Fernkommunikation lässt sich aus Art. 8 EuBagatellVO nach herrschender Auffassung jedenfalls nicht ableiten.[153] Falls eine anzuhörende Person ihren Wohnsitz in einem anderen Mitgliedstaat hat, so sind gem. Art. 8 Abs. 1 UAbs. 2 EuBagatellVO die notwendigen organisatorischen Schritte für die digitale Teilnahme dieser Person nach den Bestimmungen der EuBVO zu setzen.[154] Wurde eine Partei zu einer mündlichen Verhandlung mit persönlicher Anwesenheit geladen, so kann diese gem. Art. 8 Abs. 2 EuBagatellVO eine Teilnahme im Weg der Fernkommunikationstechnologie beantragen, sofern eine solche Technologie beim Gericht zur Verfügung steht und die durch die persönliche Anwesenheit notwendigen Vorkehrungen (insbesondere die dadurch entstehenden Kosten) in keinem angemessenen Verhältnis zur Klage stehen würden. Umgekehrt kann eine bloß zur virtuellen Teilnahme geladene Partei gem. Art. 8 Abs. 3 EuBagatellVO ihre persönliche Teilnahme bei der Verhandlung beantragen; sie riskiert in diesem Fall allerdings, gem. Art. 16 EuBagatellVO ihre dadurch entstandenen Kosten nicht ersetzt zu bekommen (worauf sie in den einschlägigen Formblättern hinzuweisen ist).[155] Entscheidungen über die Anträge nach Abs. 2 und 3 können nur mit Rechtsmitteln gegen das Urteil angefochten werden (Art. 8 Abs. 4 EuBagatellVO).[156]

### *4. Ausblick: Artikel 5 EuDigiJustVO*

Eine weitere einschlägige Neuerung wird in Bälde die Verordnung über die Digitalisierung der justiziellen Zusammenarbeit und des Zugangs zur Justiz in grenzüberschreitenden Zivil-, Handels- und Strafsachen und zur Änderung bestimmter Rechtsakte im Bereich der justiziellen Zusammenarbeit (kurz: „EuDigiJustVO")[157] brin-

---

[152] *Scheuer*, in: Fasching/Konecny, Kommentar V/3, 3. Aufl., 2023, Art. 8 EuBagatellVO Rn. 2.

[153] *Garber*, in: Geimer/Schütze, Europäisches Zivilverfahrensrecht, 4. Aufl., 2020, Art. 8 EuGFVO Rn. 1; *Mosser*, in: Geroldinger/Neumayr, IZVR II, 2021, Art. 8 EuBagVO Rn. 2; *Wolber*, in: Vorwerk/Wolf (Hrsg.), Beck'scher Online-Kommentar ZPO, 53. Aufl., 2024, Art. 8 EuGFVO Rn. 3 (Stand 1.7.2024, beck-online.de).

[154] *Mosser*, in: Geroldinger/Neumayr, IZVR II, 2021, Art. 8 EuBagVO Rn. 4; *Scheuer*, in: Fasching/Konecny, Kommentar V/3, 3. Aufl., 2023, Art. 8 EuBagatellVO Rn. 4.

[155] *Mayr*, in: Mayr, Handbuch, 2. Aufl., 2023, Rn. 12.75; *Mosser*, in: Geroldinger/Neumayr, IZVR II, 2021, Art. 8 EuBagVO Rn. 6; *Scheuer*, in: Fasching/Konecny, Kommentar V/3, 3. Aufl., 2023, Art. 8 EuBagatellVO Rn. 6.

[156] *Mayr*, in: Mayr, Handbuch, 2. Aufl., 2023, Rn. 12.75; *Mosser*, in: Geroldinger/Neumayr, IZVR II, 2021, Art. 8 EuBagVO Rn. 6.

[157] Verordnung (EU) 2023/2844 des Europäischen Parlaments und des Rates vom 13. Dezember

gen. Diese Verordnung soll die justizielle Zusammenarbeit durch Maßnahmen im Bereich der Digitalisierung stärken, indem die Kommunikation zwischen den Behörden verbessert und der Zugang zu den Behörden erleichtert wird.[158] Sie ist seit dem 16.1.2024 in Kraft und wird ab dem 1.5.2025 gelten (Art. 26 EuDigiJustVO).

Art. 5 EuDigiJustVO normiert die *Teilnahme an einer Verhandlung oder Anhörung mittels Videokonferenz- oder anderen Fernkommunikationstechnologien in Zivil- und Handelssachen:* Gem. Abs. 1 entscheidet (unbeschadet besonderer Bestimmungen in anderen Europäischen Verordnungen) eine zuständige Behörde in Verfahren in Zivil- und Handelssachen (also in aller Regel das Gericht; vgl. Art. 2 Z. 1 EuDigiJustVO) auf Antrag der Parteien oder (sofern nach deren nationalem Recht vorgesehen) von Amts wegen über die Teilnahme der Parteien und ihrer Vertreter an einer Verhandlung oder Anhörung mittels Videokonferenz oder einer anderen Fernkommunikationstechnologie. Voraussetzung dafür ist lediglich, dass sich eine der Parteien oder ihr Vertreter in einem anderen Mitgliedstaat als die Behörde aufhält. Die Behörde hat ihre Entscheidung unter Bedachtnahme auf die *Verfügbarkeit der entsprechenden Technologie* (lit. a), die *Meinung der an dem Verfahren beteiligten Parteien* zum Einsatz dieser Technologie (lit. b) sowie die *Angemessenheit des Einsatzes* dieser Technologie unter den besonderen Umständen des Einzelfalls (lit. c) zu treffen. In jedem Fall ist sicherzustellen, dass die Parteien und ihre Vertreter, einschließlich Personen mit Behinderungen, Zugang zu der Videokonferenz für die Verhandlung oder Anhörung haben (Art. 5 Abs. 2 EuDigiJustVO). Das Verfahren für die Verhandlung oder Anhörung selbst richtet sich gem. Art. 5 Abs. 4 EuDigiJustVO nach nationalem Recht.

Interessant ist in diesem Zusammenhang insbesondere, dass die Zustimmung der Parteien (anders als nach § 132a öZPO) im Anwendungsbereich der EuDigiJustVO keine Voraussetzung für die Durchführung einer digitalen oder hybriden Verhandlung darstellt, die Meinung der Parteien ist hier lediglich mitzuberücksichtigen. Dies könnte rechtspolitisch den „Türöffner" für weitere Ausdehnungen des Anwendungsbereichs des § 132a öZPO darstellen; ein echter Anpassungsbedarf des nationalen Rechts an die Vorgaben des Art. 5 EuDigiJustVO besteht meines Erachtens in Österreich allerdings nicht.

## IV. Zusammenschau

Videotechnologie ist mittlerweile ein fester Bestandteil des österreichischen Zivilverfahrens. Während Videobeweisaufnahmen bei Vorliegen der Voraussetzungen für eine Beweisaufnahme im Weg der Rechtshilfe schon seit längerem durchgeführt

2023 über die Digitalisierung der justiziellen Zusammenarbeit und des Zugangs zur Justiz in grenzüberschreitenden Zivil-, Handels- und Strafsachen und zur Änderung bestimmter Rechtsakte im Bereich der justiziellen Zusammenarbeit, ABl. L 29/1 vom 27.12.2023.

[158] ErwGr. 3 und ErwGr. 4 EuDigiJustVO; *Mayr*, in: Mayr, Handbuch, 2. Aufl., 2023, Rn. 2.51.

werden können, dehnt der mit der ZVN 2023 geschaffene § 132a Abs. 1 öZPO diese Möglichkeit für den Sachverständigenbeweis ganz allgemein und für die Vernehmung von Parteien und informierten Personen in eingeschränkter Form noch weiter aus. Gleichzeitig wurden die zunächst nur temporären Bestimmungen über die Durchführung einer Videoverhandlung (in leicht modifizierter Form) aus dem „Corona-Rechtsbestand" in das Dauerrecht überführt. Umrahmt werden diese Neuerungen durch eine verstärkte einschlägige Regelungsdichte auf Ebene des Europäischen Zivilverfahrensrechts (insbesondere in der EuBVO), wo sich die prozessökonomische „Wohltat" der Videotechnologie freilich besonders stark bemerkbar macht. Schließlich dürfte die noch nicht in Geltung stehende EuDigiJustVO den Weg für eine „Normalisierung" des Einsatzes von Videotechnologie weiter ebnen; die Entwicklung in diesem Bereich ist wohl noch (sehr) lange nicht abgeschlossen.

# Produkthaftung im digitalen Zeitalter

*Bernhard A. Koch*



## I. Was bisher geschah

Die Produkthaftung wird derzeit in allen EU-Mitgliedstaaten (sowie in jenen Ländern, die diesem Modell autonom folgen, wie etwa die Schweiz) durch die Produkthaftungsrichtlinie aus dem Jahr 1985 (im Folgenden: PHRL) geregelt.[1]

Diese Richtlinie wurde bisher nur ein einziges Mal novelliert, und zwar 1999 in Folge des BSE-Skandals, wobei alle Mitgliedstaaten nunmehr dazu verpflichtet wurden, landwirtschaftliche Erzeugnisse einzubeziehen, was bis dahin fakultativ war.[2]

Wie für EG/EU-Rechtsakte üblich, muss die Kommission regelmäßig über deren Anwendung in den Mitgliedstaaten berichten.[3] Dies gilt gemäß ihrem Art. 21 auch

[1] Richtlinie des Rates vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte (85/374/EWG), ABl. L 210/29 vom 7.8.1985.

[2] Richtlinie 1999/34/EG des Europäischen Parlaments und des Rates vom 10. Mai 1999 zur Änderung der Richtlinie 85/374/EWG des Rates zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte, ABl. L 141/20 vom 4.6.1999.

[3] Darüber hinaus wurden von der Kommission verschiedene Studien in Auftrag gegeben: *McKenna & Co*, Report for the Commission of the European Communities On the Application of Directive 85/374/EEC On Liability for Defective Products, 1994; *Fondazione Rosselli*, Analysis of the Economic Impact of the Development Risk Clause as provided by Directive 85/374/EEC on Liability for Defective Products, 2004, abrufbar unter https://ec.europa.eu/docsroom/documents/

für die PHRL, wenn auch tatsächlich in einer etwas unregelmäßigen Reihenfolge. Der allererste Bericht wurde nicht fünf, sondern erst zehn Jahre nach Verabschiedung der Richtlinie vorgelegt,[4] und der bisher letzte (fünfte) Bericht wurde 2018 veröffentlicht.[5] Dieser letzte Bericht wurde von einem Arbeitspapier der Kommissionsdienststellen begleitet,[6] in dem die Kommission zum ersten Mal seit mehr als drei Jahrzehnten offiziell bestätigte,[7] dass die Richtlinie korrekturbedürftig geworden ist (was von Wissenschaftlern und Praktikern gleichermaßen schon seit geraumer Zeit aufgezeigt worden war). In dem Arbeitspapier wird etwa ausdrücklich auf Schwierigkeiten der Opfer hingewiesen, alle Anspruchsgrundlagen zu beweisen, vor allem aber auch auf die mangelnde Eignung des aktuellen Richtlinien-Wortlauts für Produkte mit neuen digitalen Technologien.[8]

---

7104 (Abrufdatum: 30.7.2024); *Lovells*, Die Produkthaftung in der Europäischen Union. Ein Bericht für die Europäische Kommission, 2003, abrufbar unter https://ec.europa.eu/docsroom/documents/7106 (Abrufdatum: 30.7.2024) sowie *European Commission*, Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products – Final report, 2018, abrufbar unter https://data.europa.eu/doi/10.2873/477640 (Abrufdatum: 30.7.2024).

[4] Erster Bericht über die Anwendung der Ratsrichtlinie zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte (85/374/EWG), Brüssel, den 13.12.1995, KOM(95)617 endg.; Green Paper Liability for defective products, Brussels, 28.7.1999, COM(1999)396 final; Bericht der Kommission über die Anwendung der Richtlinie 85/374 über die Haftung für fehlerhafte Produkte, Brüssel, den 31.1.2001, KOM(2000) 893 endg.; Dritter Bericht über die Anwendung der Richtlinie des Rates zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte (85/374/EWG vom 25.7.1985, geändert durch die Richtlinie 1999/34/EG des Europäischen Parlaments und des Rates vom 10.5.1999), Brüssel, den 14.9.2006, KOM(2006) 496 endg.; Vierter Bericht über die Anwendung der Richtlinie 85/374/EWG des Rates zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte, geändert durch die Richtlinie 1999/34/EG des Europäischen Parlaments und des Rates vom 10.5.1999, Brüssel, den 8.9.2011, KOM(2011) 547 endg.; sowie der in der nächsten Fn. zitierte Fünfte Kommissionbericht. Siehe auch das Grünbuch: Die zivilrechtliche Haftung für fehlerhafte Produkte, Brüssel, den 28.7.1999, KOM(1999) 396 endg.

[5] Bericht der Kommission an das Europäische Parlament, den Rat und den Europäischen Wirtschafts- und Sozialausschuss über die Anwendung der Richtlinie des Rates zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte (85/374/EWG), Brüssel, den 7.5.2018, COM(2018) 246 final.

[6] Commission Staff Working Document: Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, Brussels, 7.5.2018, SWD(2018) 157 final.

[7] Siehe z. B. die Beiträge zu Machnikowski (Hrsg.), European Product Liability: An Analysis of the State of the Art in the Era of New Technologies, 2016.

[8] „There are, however, certain aspects of the Directive that have an impact on the effectiveness of the Directive. There are concerns about […] the burden of proof. At present, it appears that especially complex products […] pose a problem […] that may make it very difficult for consumers to be able to prove the links between defects and damages. […] Furthermore, the definition of product appears to no longer be as clear-cut as it may have been when the Directive was adopted for example in the light of new technological developments where the distinction between products and services becomes blurred or in the context of software.“, siehe Commission Staff Working Document (Fn. 6), 61.

Der fünfte Kommissionsbericht kam daher selbst zu dem Ergebnis, dass die Richtlinie in ihrer jetzigen Form möglicherweise nicht mehr perfekt ist und dass einige Kernelemente (insbesondere die Frage, welche Produkte unter die Regelung fallen) wohl überdacht oder zumindest geklärt werden müssen. Auch hier wurde die Beweislast als besonderer Problemfall hervorgehoben, zumindest wenn es um „komplexe" Produkte wie digitale oder pharmazeutische Produkte geht.[9]

Zeitgleich mit ihrem fünften Bericht kündigte die Kommission die Einrichtung einer Expertengruppe für Haftung und neue Technologien an, die im selben Jahr mit zwei Untergruppen ins Leben gerufen wurde.[10] Die erste Untergruppe (mit der Bezeichnung „*Product Liability Formation*", PLF) wurde – wenig überraschend – damit beauftragt, sich speziell mit der Produkthaftungsrichtlinie zu befassen und zu prüfen, ob diese geändert werden muss. Sie setzte sich aus Vertretern der Mitgliedstaaten und bestimmter Interessensgruppen sowie einigen Akademikern zusammen. Die „*European Group on Tort Law*" war ebenfalls Mitglied dieser Untergruppe.[11] Die zweite Untergruppe war die „*New Technologies Formation*" (NTF), die sich deutlich von der ersten unterschied. Zunächst einmal war ihre Mitgliedschaft auf Wissenschaftlerinnen und Wissenschaftler beschränkt.[12] Außerdem war die Aufgabe der NTF viel breiter gefasst – sie sollte sich grundsätzlicher mit den Herausforderungen neuer digitaler Technologien für das Deliktsrecht im Binnenmarkt befassen und eine Art Masterplan für allfällige legistische Maßnahmen ausarbeiten.[13] Ein Grund für die Aufteilung zwischen den beiden Untergruppen war die interne Arbeitsteilung in der Kommission. Die Produkthaftung fiel (und fällt) in den Zuständigkeitsbereich der GD GROW,[14] während die übrigen Haftungsfragen der GD JUST zugewiesen sind.[15]

---

[9] „Die Richtlinie deckte bislang eine breite Palette von Produkten und technologischen Entwicklungen ab. Sie ist grundsätzlich ein nützliches Instrument […] Dies bedeutet nicht, dass die Richtlinie perfekt ist. Ihre Wirksamkeit wird durch Konzepte (wie ‚Produkt', ‚Hersteller', ‚Fehler', ‚Schaden' oder die Beweislast) beeinträchtigt, die in der Praxis wirksamer sein könnten. […] Dies gilt insbesondere dann, wenn die Beweislast komplex ist, wie dies bei einigen neuen digitalen Technologien oder bei Arzneimitteln der Fall sein kann.", siehe Fünfter Kommissionsbericht (Fn. 5), 9 f.

[10] Abrufbar unter https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups consult?lang=de&do=groupDetail.groupDetail&groupID=3592 (Abrufdatum: 30.7.2024).

[11] Der Autor ist Mitglied dieser Arbeitsgruppe, abrufbar unter http://www.egtl.org (Abrufdatum: 30.7.2024).

[12] Der Autor war Mitglied dieser Untergruppe (NTF).

[13] Wie die Ausschreibung sagte, solle die NTF „assess whether and to what extent existing liability schemes are adapted to the emerging market realities following the development of the new technologies such as Artificial Intelligence, advanced robotics, the IoT and cybersecurity issues. It shall identify the shortcomings and […] assist the Commission in developing EU-wide principles which can serve as guidelines for possible adaptations of applicable laws at EU and national level as regards the new technologies […]".

[14] Generaldirektion Binnenmarkt, Industrie, Unternehmertum und KMU.

[15] Generaldirektion Justiz und Verbraucher. Neben der GD JUST war die NTF auch der GD GROW sowie der Generaldirektion Kommunikationsnetze, Inhalte und Technologien („GD Connect") zugeordnet.

Die NTF präsentierte ihren Abschlussbericht 2019,[16] während die PLF nie einen Bericht vorlegte. Dies ist in erster Linie darauf zurückzuführen, dass es in dieser Untergruppe keine Einigung darüber gab, was überhaupt mit der PHRL geschehen sollte. Die PLF beendete ihre Arbeit mit einem Patt, bei dem das einzig denkbare Ergebnis eher ein Leitfaden von fragwürdiger rechtlicher Relevanz als tatsächliche Änderungen am Wortlaut der Richtlinie zu sein schien, oder – wie ein Mitglied der PLF es nannte – ein „*idiots' guide to the Directive*".[17]

In der Zwischenzeit wurde der politische Druck auf die Kommission immer größer,[18] sich mit Haftungsfragen im Zusammenhang mit KI, Robotik und dergleichen zu befassen. Sie veröffentlichte daher u. a. im Jahr 2020 einen Bericht,[19] in dem sie auf mögliche Schwierigkeiten für Opfer solcher neuen Technologien hinwies, im Rahmen der bestehenden Haftungsregelungen eine Entschädigung zu erhalten. Erstmals wurde darin auch offiziell darauf hingewiesen, dass es möglicherweise notwendig ist, den Wortlaut der PHRL selbst zu ändern.[20] Die Kommission bat daraufhin im Rahmen einer öffentlichen Konsultation um weiteres Feedback dazu.[21]

Neben den laufenden Arbeiten der Kommission hatte das *European Law Institute* (ELI) das Thema aufgegriffen und mehrere Dokumente veröffentlicht, neben einer Antwort auf die besagte Konsultation[22] etwa die 2021 von *Christian Twigg-Flesner*

---

[16] Liability for artificial intelligence and other emerging digital technologies, abrufbar unter https://data.europa.eu/doi/10.2838/573689 (Abrufdatum: 30.7.2024). Siehe dazu das Sonderheft des Journal of European Tort Law (JETL) zu diesem Bericht: JETL 2020, Vol. 11 Iss. 2, 115.

[17] Protokoll des PLF-Treffens vom 18.2.2019, abrufbar unter https://ec.europa.eu/transparency/expert-groups-register/core/api/front/document/31014/download (Abrufdatum: 30.7.2024), 2.

[18] Ausgehend unter anderem vom Europaparlament, das nach seiner Entschließung vom 16.2.2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103(INL)), ABl. C 252/239 vom 18.7.2018, einen Vorschlag für eine Verordnung (!) „über Haftung für den Betrieb von Systemen mit künstlicher Intelligenz" vorgelegt hatte: Entschließung des Europäischen Parlaments vom 20.10.2020 mit Empfehlungen an die Kommission für eine Regelung der zivilrechtlichen Haftung beim Einsatz künstlicher Intelligenz (2020/2014(INL)), ABl. C 404/107 vom 6.10.2021.

[19] Bericht der Kommission an das Europäische Parlament, den Rat und den Europäischen Wirtschafts- und Sozialausschuss: Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung, Brüssel, den 19.2.2020, COM(2020) 64 final (zusammen mit anderen Dokumenten zur KI vom selben Tag).

[20] „Grundsätzlich sind die bestehenden Haftungsvorschriften der Union und der Mitgliedstaaten auch für neue Technologien geeignet, doch könnte es […] schwieriger werden, Opfer von Schäden in allen Fällen, in denen dies gerechtfertigt wäre, zu entschädigen. […] Um hier Abhilfe zu schaffen und mögliche Unsicherheiten im bestehenden Rechtsrahmen zu beseitigen, könnten bestimmte Anpassungen der Produkthaftungsrichtlinie und der nationalen Haftungsregelungen durch geeignete EU-Initiativen auf der Grundlage eines gezielten, risikobasierten Ansatzes […] in Erwägung gezogen werden." Bericht 2020 (Fn. 19), 20 f.

[21] Abrufbar unter https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Produkthaftungsrichtlinie-Anpassung-der-Haftungsvorschriften-an-das-digitale-Zeitalter-die-Kreislaufwirtschaft-und-globale-Wertschopfungsketten_de (Abrufdatum: 30.7.2024).

[22] Abrufbar unter https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_European_Commission_s_Public_Consultation_on_Civil_Liability_Adapting_Liability_Rules_to_the_Digital_Age_and_Artificial_Intelligence.pdf (Abrufdatum: 30.7.2024).

verfassten „*Guiding Principles for Updating the Product Liability Directive for the Digital Age*“.[23] Auf Initiative der wissenschaftlichen Direktorin des ELI, *Christiane Wendehorst*, erstellte das ELI 2022 sogar einen kompletten Entwurf einer überarbeiteten Richtlinie.[24] Zum Zeitpunkt seiner Veröffentlichung war jedoch bereits klar, dass die Kommission zeitnah ihren eigenen neuen Entwurf vorlegen würde. Die Kommission veröffentlichte einen solchen Vorschlag tatsächlich am 28.9.2022, in dem sie nicht nur Änderungen an der alten Richtlinie vorschlug, sondern diese vollständig durch eine neue Richtlinie ersetzen wollte.[25]

Am selben Tag wurde eine weitere neue Richtlinie vorgeschlagen, die kurz „KI-Haftungsrichtlinie“[26] genannt wurde, obwohl diese offizielle Kurzbezeichnung unpassend ist. Dieser zweite Entwurf enthielt nämlich keine wirkliche Regelung von Haftungsgründen (geschweige denn ein umfassendes Regelwerk), sondern wollte lediglich – aber immerhin – die bestehenden nationalen Verschuldenshaftungsregelungen in allen Mitgliedstaaten um einheitliche (Mindest-)Vorschriften zur Feststellung und zur Beweislast ergänzen, diese aber ansonsten unangetastet lassen, so dass die harmonisierende Wirkung dieses zweiten Richtlinienvorschlags in der Praxis eher gering wäre. Das Los dieses zweiten Entwurfs ist noch unklar. Er wurde sofort auf Eis gelegt, allein schon wegen des zu dieser Zeit noch unklaren Schicksals des damaligen Entwurfs eines „Gesetzes über künstliche Intelligenz“,[27] auf das der Entwurf ausführlich Bezug nimmt. Nun, da die (nunmehr) KI-Verordnung verabschiedet wurde,[28] bleibt abzuwarten, ob dieser zweite Entwurf irgendwann doch noch wiederbelebt wird.[29]

---

[23] Abrufbar unter https://europeanlawinstitute.eu/projects-publications/publications/eli-innovation-paper-guiding-principles-for-updating-the-product-liability-directive-for-the-digital-age/ (Abrufdatum: 30.7.2024).

[24] *European Law Institute*, ELI Draft of a Revised Product Liability Directive, Draft Legislative Proposal of the European Law Institute, abrufbar unter https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Draft_of_a_Revised_Product_Liability_Directive.pdf (Abrufdatum: 30.7.2024).

[25] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Haftung für fehlerhafte Produkte, Brüssel, den 28.9.2022, COM(2022) 495 final. Siehe dazu auch die Stellungnahme des ELI zu diesem Entwurf, abrufbar unter https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Feedback_on_the_EC_Proposal_for_a_Revised_Product_Liability_Directive.pdf (Abrufdatum; 30.7.2024).

[26] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz (Richtlinie über KI-Haftung), Brüssel, den 28.9.2022, COM(2022) 496 final.

[27] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, Brüssel, den 21.4.2021, COM(2021) 206 final.

[28] Zum Zeitpunkt des Abschlusses des Manuskripts war nur noch die Veröffentlichung im Amtsblatt ausständig: Verordnung (EU) 2024/[…] des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz).

[29] Zum Zeitpunkt des Abschlusses des Manuskripts gab es bereits eine entsprechende (zurückhaltende) Diskussion in einer Ratsarbeitsgruppe.

Die Zukunft des Entwurfs einer neuen PHRL (im Folgenden NPHRL) war jedoch von Anfang an aussichtsreicher. In der Tat wurde er von den meisten Mitgliedstaaten und Interessengruppen recht positiv aufgenommen, sodass sein Weg durch die Gesetzgebungspipeline erstaunlich schnell verlief. Eine politische Einigung im Rat wurde bereits unter der spanischen Präsidentschaft 2023 erzielt, und auch das Parlament stimmte – trotz anfänglicher Anzeichen möglicher Stolpersteine – Ende Dezember desselben Jahres verhältnismäßig schnell zu. Der Ausschuss der Ständigen Vertreter (COREPER) bestätigte diese Einigung einen Monat später.[30] Die jüngste Entwicklung zum Zeitpunkt der Schriftlegung dieses Beitrages ist die offizielle Annahme einer legislativen Entschließung durch das Parlament am 12.3.2024.[31] Diese Textfassung der NPHRL wird im Folgenden verwendet (und nicht der ursprüngliche Kommissionsvorschlag), auch wenn bis zur Endfassung noch geringfügige stilistische Anpassungen möglich sind.[32]

## II. Vorgeschlagene Änderungen der PHRL

Es sieht zum Zeitpunkt des Abschlusses dieses Manuskripts so aus, als würde der Entwurf von 2022 noch im Jahr 2024 verabschiedet werden (vorbehaltlich möglicher technischer Verzögerungen). Doch was wird die neue Richtlinie bewirken? Sie wird die alte PHRL zwar vollständig ersetzen und nicht nur punktuell ändern, aber ein Großteil des ursprünglichen Textes und der Konzepte bleibt dennoch erhalten, trotz einiger bedeutender Änderungen, die im Folgenden überblickshaft dargestellt werden.

### *1. Ersatzfähige Schäden*

Beginnen wir dort, wo alle Schadenersatzfälle beginnen – bei der Frage, welche Schäden durch die neue Regelung tatsächlich abgedeckt werden. Die derzeitige PHRL ist auf Personenschäden (einschließlich tödlicher Verletzungen) und bestimmte Sachschäden beschränkt. Daran wird sich im Wesentlichen nichts ändern, wenn auch mit einigen Verfeinerungen und geringfügigen Ausweitungen zu rechnen ist.

---

[30] Abrufbar unter https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5809_2024_INIT (Abrufdatum: 30.7.2024).

[31] Legislative Entschließung des Europäischen Parlaments vom 12. März 2024 zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Haftung für fehlerhafte Produkte (COM(2022)0495 – C9-0322/2022 – 2022/0302(COD)).

[32] Mittlerweile wurde die NPHRL verabschiedet; die Zitate im Folgenden entsprechen aber der Endfassung: RL (EU) 2024/2853 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über die Haftung für fehlerhafte Produkte und zur Aufhebung der Richtlinie 85/374/EWG des Rates, ABl L 2024/2853 vom 18.11.2024.

*a) Körperschäden und Tötung*

Selbstverständlich wird auch die NPHRL Körperschäden und Todesfälle erfassen, und die ausdrückliche Erwähnung „medizinisch anerkannter Beeinträchtigungen der psychischen Gesundheit" in Art. 6 Abs. 1 lit. a NPHRL ist eher eine Klarstellung als eine wirkliche Erweiterung. Nach einigen Diskussionen wird in Art. 6 Abs. 2 NPHRL nun ausdrücklich bestätigt, dass die Mitgliedstaaten neben materiellen auch immaterielle Schäden kompensieren können, allerdings nur dann, wenn diese Folge der in Abs. 1 genannten Schäden,[33] also Sekundärschäden sind, und auch dann nur, wenn es dafür im Recht des betroffenen Mitgliedstaates auch in anderen Haftungsfällen Ersatz gibt.

*b) Sachschäden*

Wichtiger sind beim künftigen Schadensbegriff aber die Anpassungen bei den Sachschäden, die gedeckt werden sollen. Es konnte endlich eine Einigung erzielt werden, um die von Anfang an umstrittene 500-Euro-Untergrenze abzuschaffen.[34] Dieses Limit war in den Mitgliedstaaten ohnehin unterschiedlich ausgelegt worden; einige sahen sie als bloßen Schwellenwert, andere als Selbstbeteiligung.[35]

An den Grenzen der erstattungsfähigen Sachschäden wurde aber noch weiter nachjustiert. Insbesondere wurde der bislang etwas zweideutige Ausschluss von Schäden an beruflich genutzten Gegenständen[36] nun auf Sachen beschränkt, die ausschließlich zu solchen Zwecken genutzt werden.[37] Vermögensgegenstände mit doppeltem Verwendungszweck, wie z. B. ein Notebook, das sowohl für berufliche als auch für private Zwecke genutzt wird, sind nun ausdrücklich durch die neue Regelung geschützt, wenn sie durch ein fehlerhaftes Produkt beschädigt werden.

Ein weiterer Teil der Neudefinition des ersatzfähigen Sachschadens ist m. E. unglücklich. Zumindest stellt aber Art. 6 Abs. 1 lit. b sublit. ii NPHRL ein für alle Mal klar, dass das, was wir als „Weiterfresserschäden" bezeichnen,[38] nicht aus Produkt-

---

[33] Damit sind aber auch immaterielle Schäden in Folge (!) von Sach- oder Datenschäden grundsätzlich mitumfasst, sofern die Mitgliedstaaten auch sonst dafür Ersatz vorsehen.

[34] Siehe nur EuGH, Urt. v. 25.4.2002 – Rs. C-52/00 (Kommission/Frankreich); dazu *B.A. Koch*, European Union, in: Koziol/Steininger (Hrsg.), European Tort Law 2002, 2003, 432 (450 ff., insbesondere 451 ff.).

[35] Siehe z. B. dritter Kommissionsbericht (Fn. 4), 11.

[36] Bislang musste die beschädigte Sache gem. Art. 9 lit. b PHRL zwei Voraussetzungen erfüllen: Sie musste „von einer Art" sein, „wie sie gewöhnlich für den privaten Ge- oder Verbrauch bestimmt ist," und (kumulativ!) „von dem Geschädigten hauptsächlich zum privaten Ge- oder Verbrauch verwendet worden" sein. Durch die sehr freihändige Übersetzung dessen in § 2 Z. 2 PHG (ein Sachschaden ist ersatzfähig, wenn ihn „nicht ein Unternehmer erlitten hat, der die Sache überwiegend in seinem Unternehmen verwendet hat") war die österreichische Umsetzung bislang wahrscheinlich mangelhaft: *Koziol/Apathy/B.A. Koch*, Österreichisches Haftpflichtrecht III, 3. Aufl., 2014, Rn. B/100 ff.

[37] Art. 6 Abs. 1 lit. b sublit. iii NPHRL.

[38] *Koziol/Apathy/B.A. Koch*, Haftpflichtrecht III, 3. Aufl., Rn. B/96 ff.

haftung kompensiert werden kann. Wenn ein Auto mit mangelhaften Reifen ausgeliefert wird und deshalb einen Unfall erleidet, ist der Schaden am Rest der Welt natürlich gedeckt, nicht aber der Schaden am Auto selbst. Das ergibt Sinn, wenn es um Klagen gegen den Autohersteller geht (also den Hersteller des Endprodukts, das die von Dritten beigesteuerten Komponenten „Reifen" mitumfasst), aber nicht so sehr, wenn man bedenkt, dass der Eigentümer des beschädigten Fahrzeugs stattdessen Schadenersatz vom Reifenhersteller als Verursacher des fehlerhaften Bauteils verlangen könnte. Wären die Reifen getrennt verkauft worden (auch wenn sie in derselben Charge hergestellt worden sind), könnte der Fahrzeugeigner dies natürlich sehr wohl tun, weil dann die Reifen die Endprodukte wären.

*c) Schäden an „Daten"*

Eine Schadensart, die in der Liste von aus Produkthaftung ersatzfähigen Schäden tatsächlich neu ist, ist die Zerstörung oder Beschädigung von Daten. Diese sind derzeit wohl nicht abgedeckt, zumindest wenn man davon ausgeht, dass der Begriff der „Sache" in Art. 9 lit. b PHRL auf körperliche Gegenstände beschränkt ist. Der entsprechende Zusatz in Art. 6 Abs. 1 lit. c NPHRL ist daher wichtig. Es ist jedoch bedauerlich, dass die bereits erwähnte Verbesserung der PHRL in Bezug auf beschädigte körperliche Sachen (mit Beantwortung der Frage des *dual use* zu Gunsten der Geschädigten) nicht auf Daten ausgedehnt wurde – Dateien[39] sind nach der neuen Regelung somit nur geschützt, wenn sie „nicht zu beruflichen Zwecken verwendet werden", ohne den Zusatz „ausschließlich".

*d) (Weiterhin) nicht erfasste Schäden*

Die neue EU-Produkthaftungsregelung deckt nach wie vor keine reinen Vermögensschäden ab, und auch selbstständige emotionale oder andere (primäre) immaterielle Schäden werden nicht erfasst.[40] Dies ist insbesondere im Hinblick auf die Ausweitung der neuen Regelung auf KI wichtig,[41] die eine ganze Reihe solcher Schäden auslösen kann. Man denke nur an eine Rekrutierungssoftware basierend auf einer KI, die aus dem Ruder gelaufen ist und diskriminierend wurde. Der daraus resultierende Verlust des zu Unrecht ausgeschlossenen Stellenbewerbers fällt nicht unter das künftige NPHRL-Regime.

---

[39] Es ist schade, dass der Wortlaut der NPHRL beim Begriff „Daten" verhaftet bleibt (und diesen in Art. 2 Abs. 4 NPHRL definiert). (Jedenfalls) um Verwechslung mit dem Datenbegriff der DSGVO zu vermeiden, wäre es besser gewesen, man hätte stattdessen von „Dateien" gesprochen. Dazu *B.A. Koch*, Dateischäden, in: FS für Peter Bydlinski, 2022, 545.

[40] Die in Art. 6 Abs. 2 NPHRL genannten „immateriellen Verluste" müssen sich „aus dem in Absatz 1 genannten Schaden ergeben", damit sie ersetzt werden können, also indirekte (sekundäre) Folge der in Abs. 1 aufgelisteten (primären) Schadensarten sein (Körper-, Sach- oder Datenschäden).

[41] Dazu sogleich unter 2.b.

### *2. Produktbegriff*

#### *a) Produkte in der derzeitigen Richtlinie*

Gegenwärtig sind nur „bewegliche Sachen" Produkte im Sinne der PHRL,[42] und obwohl zusätzlich noch ausdrücklich Elektrizität genannt wird, ist die überwiegende Meinung der Ansicht, dass der Produktbegriff der PHRL auf körperliche Gegenstände beschränkt ist (obwohl diese Einschränkung im Wortlaut fehlt),[43] wodurch unter anderem Software ausgeschlossen wird, zumindest wenn sie gesondert verkauft wird.[44]

Eine offizielle Erklärung der Kommission aus dem Jahr 1988, dass die Richtlinie „auf Computer-Software Anwendung" findet,[45] scheint dem auf den ersten Blick zu widersprechen. Dabei muss man aber bedenken, dass damals Software noch nicht direkt online verkauft wurde, sondern stets auf körperlichen Datenträgern wie Festplatten oder Disketten, und diese waren die eigentlichen (aber eben körperliche) Produkte, die als solche aufgrund der darauf vorinstallierten Software fehlerhaft wurden.[46]

#### *b) Produkte in der künftigen Richtlinie*

Der neue Wortlaut behält den Begriff der „beweglichen Sachen" in der Produktdefinition bei, fügt jedoch in Art. 4 Z. 1 NPHRL an den von der bisherigen PHRL übernommenen Begriff „Elektrizität" nun ausdrücklich „digitale Bauunterlagen, Rohstoffe und Software" hinzu. Was die Rohstoffe betrifft, so ist dies nichts Neues (auch wenn es derzeit an anderer Stelle in der Richtlinie erwähnt wird).[47]

„Digitale Bauunterlagen" („*digital manufacturing files*" in der englischen Fassung) werden noch im selben Artikel definiert.[48] Im Wesentlichen handelt es sich dabei um Dateien zur Verwendung mit 3D-Druckern oder vergleichbaren Geräten, die etwas

---

[42] Art. 2 PHRL lautet: „Bei der Anwendung dieser Richtlinie gilt als ‚Produkt' jede bewegliche Sache, auch wenn sie einen Teil einer anderen beweglichen Sache oder einer unbeweglichen Sache bildet. Unter ‚Produkt' ist auch Elektrizität zu verstehen."

[43] In der österreichischen Umsetzung wurde sie aber „freihändig" in § 1 Abs. 1 PHG ergänzt; dazu *Koziol/Apathy/B.A. Koch*, Haftpflichtrecht III, 3. Aufl., Rn. B/116.

[44] Vgl. z. B. *Machnikowski*, Conclusions, in: Machnikowski (Hrsg.), European Product Liability: An Analysis of the State of the Art in the Era of New Technologies, 2016, 669 (693).

[45] ABl. C 114/89 vom 8.5.1989.

[46] Insoweit kann Software natürlich auch heute schon eine Produkthaftung auslösen, aber das fehlerhafte Produkt ist dabei nur der körperliche Datenträger, nicht die Software selbst. Somit haftet der Hersteller des Datenträgers, nicht der Entwickler der Software.

[47] Art. 3 Abs. 1 PHRL definiert den Produzenten u. a. als den „Hersteller […] eines Grundstoffs oder eines Teilprodukts".

[48] Art. 4 Z. 2 NPHRL definiert „digitale Bauunterlagen" als „digitale Version einer beweglichen Sache oder eine digitale Vorlage dafür, die funktionale Informationen enthält, die zur Herstellung eines materiellen Gegenstands erforderlich sind, indem sie die automatische Steuerung von Maschinen oder Werkzeugen ermöglicht".

Körperliches auf der Grundlage von vorab von einem Dritten definierten (und separat vertriebenen) digitalen Fertigungsspezifikationen erzeugen.

Software hingegen ist nirgends in der neuen Richtlinie definiert. In den Erwägungsgründen werden allerdings Beispiele genannt, so etwa Betriebssysteme, Anwendungen und – ausdrücklich – auch KI-Systeme (ErwGr. 13). *Open Source Software* ist jedoch in Art. 2 Abs. 2 NPHRL vom Anwendungsbereich der neuen Richtlinie ausgeschlossen, sofern „außerhalb einer gewerblichen Tätigkeit entwickelt oder bereitgestellt". Die Erwägungsgründe stellen klar, dass die Art des Software-Erwerbs irrelevant ist – Downloads über das Internet sind ebenso eingeschlossen wie Vertrieb als *Software-as-a-Service*.[49] Das ergibt natürlich Sinn – es kann und sollte keinen Unterschied machen, ob jemand etwa Office-Software zur dauerhaften lokalen Installation kauft (die aber ohnehin regelmäßig aktualisiert wird) oder stattdessen dieselbe Software abonniert, die in einer ständig aktualisierten Version online zur Verfügung gestellt wird.

*c) „Komponenten"*

Eine noch radikalere Ausweitung erfolgt durch die neue Definition von „Komponenten" in Art. 4 Z. 4 NPHRL.[50] Der Hersteller eines fehlerhaften Bau- oder Bestandteils einschließlich im Endprodukt verarbeiteter Rohmaterialien haftet natürlich schon jetzt direkt nach der bestehenden PHRL-Regelung neben dem Hersteller des fertigen Produkts,[51] sofern der Fehler desselben aus dem verarbeiteten Teil ausging.[52]

Künftig umfasst der Begriff „Komponente" aber nicht nur unkörperliche Sachen (was die logische Folge der Einbeziehung von Software als Endprodukt ist), sondern er wird auch auf damit „verbundene Dienste" ausgedehnt. Ein „verbundener Dienst" wird in Art. 4 Z. 3 NPHRL definiert als „digitale[r] Dienst, der so in ein Produkt integriert oder so mit ihm verbunden ist, dass das Produkt ohne ihn eine oder mehrere seiner Funktionen nicht ausführen könnte". Dies ist eine noch weiter gehende Abweichung von der ursprünglichen Beschränkung auf körperliche Fertigprodukte durch die Einbeziehung von Software. Immerhin geht zumindest die derzeitige PHRL von einem Hersteller aus, der ein Produkt fertigstellt und in Verkehr bringt und damit dessen Schicksal ab dann anderen überlässt. Zu diesem Zeitpunkt haben die Komponentenhersteller längst ihren Beitrag geleistet. Ein Anbieter einer damit zusammenhängenden „verbundenen" Dienstleistung hingegen beginnt seinen Beitrag erst *nach*

---

[49] ErwGr. 13 stellt klar, dass Software erfasst ist „unabhängig davon, ob die Software auf einem Gerät gespeichert oder über ein Kommunikationsnetz oder Cloud-Technologien abgerufen oder durch Software als Dienstleistung bereitgestellt wird".

[50] „Komponente" bezeichnet demzufolge „jeden materiellen oder immateriellen Gegenstand oder Rohstoff und jeden verbundenen Dienst, der in das Produkt integriert oder mit dem Produkt verbunden wird".

[51] Hersteller „eines Grundstoffes oder eines Teilprodukts" werden bereits bisher in Art. 3 Abs. 1 PHRL ausdrücklich als mögliche Beklagte neben dem Endhersteller genannt.

[52] *Koziol/Apathy/B.A. Koch*, Haftpflichtrecht III, 3. Aufl., Rn. B/241 ff.

dem Vertrieb des Produkts und erbringt ab dann weiterhin Dienstleistungen, die nach der alten Regelung überhaupt ausdrücklich ausgeschlossen waren.

In den Erwägungsgründen werden als Beispiele für verbundene Dienste u. a. Navigations- oder Sprachassistenzsysteme genannt.[53] Ausdrücklich ausgeschlossen werden aber reine Internetzugangsdienste (die allerdings natürlich zwangsläufig zumeist erforderlich sind, um solche digitalen Dienste tatsächlich zu erbringen).[54]

In Anbetracht der Tatsache, dass der bloße Inhalt digitaler Dateien als solcher nicht unter den Begriff der „Software" fallen soll und daher ausgeschlossen ist,[55] wird sich die Rechtsprechung des EuGH künftig mit verschiedenen unvermeidlichen Grenzfragen befassen müssen. Wie schaut es etwa mit einem „Navigationssystem" aus (ein ausdrücklich genannter verbundener Dienst) – ist damit lediglich dessen Funktionalität zur Berechnung einer Route gemeint, oder sind doch auch die zugrunde liegenden Kartendaten (die auf den ersten Blick unter den Begriff „Inhalt" zu fallen scheinen) umfasst? Das eine funktioniert ohne das andere nicht, Fehler des einen wirken sich auf das Ergebnis seines Zusammenspiels mit dem anderen aus.

### *d) Beispiele*

#### *aa) Auto*

Nehmen wir das Beispiel eines Autos als Endprodukt, das natürlich bereits jetzt unter die bestehende PHRL-Regelung fällt. Dieses Auto besteht aus verschiedenen körperlichen Bauteilen, hat aber schon seit langem eine Menge Software vorinstalliert, von der einige bereits jetzt KI-basiert sein können. Der Hersteller des fertigen Produkts stellt in der Regel eine Art *Backend*-System zur Verfügung, das den Betrieb des Fahrzeugs unterstützt. Auf mein eigenes Auto kann ich zum Beispiel über mein Smartphone aus der Ferne zugreifen, und das ist ein Dienst, der zumindest indirekt vom Hersteller meines Fahrzeugs angeboten und betrieben wird. Um den Dienst zu nutzen, braucht es eine aufrechte Online-Kommunikation in beide Richtungen. Denkbar sind auch noch Drittanbieter, die Unterstützung i. w. S. für das Fahren an-

---

[53] „Beispiele für verbundene Dienste sind die kontinuierliche Bereitstellung von Verkehrsdaten in einem Navigationssystem, ein Gesundheitsüberwachungsdienst, der sich auf die Sensoren eines physischen Produkts stützt, um die körperliche Aktivität oder Gesundheitsparameter des Nutzers nachzuverfolgen, eine Temperaturüberwachung, die die Temperatur eines intelligenten Kühlschranks überwacht und reguliert, oder auch ein Sprachassistent, der die Steuerung eines oder mehrerer Produkte mittels Sprachbefehlen ermöglicht." (ErwGr. 17).

[54] „Internetzugangsdienste sollten nicht als verbundene Dienste behandelt werden, da sie nicht als Teil eines Produkts angesehen werden können, das der Kontrolle eines Herstellers unterliegt, und es wäre unangemessen, die Hersteller für Schäden haftbar zu machen, die durch Mängel bei Internetzugangsdiensten verursacht werden. Allerdings könnte ein Produkt, das sich auf Internetzugangsdienste stützt und bei einer Verbindungsunterbrechung keine Sicherheit gewährleisten kann, als fehlerhaft im Sinne dieser Richtlinie eingestuft werden." (ErwGr. 17).

[55] „Informationen sind jedoch nicht als Produkt zu betrachten, und die Produkthaftungsvorschriften sollten daher nicht für den Inhalt digitaler Dateien wie Mediendateien oder E-Books oder den Quellcode von Software gelten." (ErwGr. 13).

bieten, z. B. Anbieter von Navigationsdiensten oder zumindest von Kartenupdates dafür. Die meisten dieser Dienste[56] fallen unter den Begriff der „verbundenen Dienste" i. S. d. Art. 4 Z. 3 NPHRL, während die Erwägungsgründe den Internetdienstanbieter, der die verschiedenen Komponenten verbindet, ausdrücklich ausnehmen.

*bb) Smartphone-App*

Nehmen wir nun statt einem körperlichen Endprodukt wie das Auto aus dem vorherigen Beispiel ein rein digitales Produkt, etwa eine Hautkrebs-Screening-App. Mit solcher schon jetzt vertriebener Software kann man sichtbare Veränderungen der Haut selbst untersuchen, indem Fotos davon mit einem KI-gesteuerten Datenbankvergleich überprüft werden. Die App meldet dann zurück, ob es sich beim visuell Begutachteten um gut- oder bösartige Veränderungen handeln könnte.

Die App enthält natürlich keine körperlichen Komponenten wie das Auto, besteht aber jedenfalls aus einem Code, der zumindest Verbindungen zu KI-Algorithmen enthält. Der Betrieb der App erfordert wenigstens einen oder vielleicht sogar mehrere *Backend*-Dienste (insbesondere natürlich den Zugriff auf die Melanom-Datenbank), die für den Abgleich der eigenen Bildaufnahmen und damit für das planmäßige Funktionieren der App unerlässlich sind. Bei diesen Diensten handelt es sich – wiederum – um „verbundene Dienste" i. S. d. Art. 4 Z. 3 NPHRL, da ohne sie der Hauptzweck der App, für den sie konzipiert wurde, nicht erfüllt werden könnte.

Das Problem ist jedoch, dass man die App nicht ohne einen körperlichen Gegenstand betreiben kann, in diesem Fall typischerweise ein Smartphone, das in der Regel weder vom App-Entwickler selbst hergestellt noch bereitgestellt wird. Das Smartphone selbst verfügt natürlich über verschiedene körperliche und unkörperliche Komponenten (wie Firm- oder Software).

Eine falsche Antwort der App kann entweder auf einen Fehler in der App selbst (also im Endprodukt) oder auf einen Fehler im (damit verbundenen Dienst) *Backend*-System zurückzuführen sein, was künftig alles unter die NPHRL fällt. Der App-Entwickler kann aber zur Abwehr von Ansprüchen behaupten, dass die App selbst und die damit verbundenen Dienste einwandfrei funktioniert haben, jedoch das vom Smartphone aufgenommene Bild so fehlerhaft war, dass die App keine andere Wahl hatte, als eine objektiv falsche Antwort zu liefern. Das Smartphone und seine Kamera liegen dabei natürlich nicht in der Kontrolle des App-Entwicklers und waren es auch nie. Daraus resultierende Probleme für das Opfer beim Kausalitätsnachweis werden nur geringfügig durch die neuen Beweisregeln[57] abgemildert.

---

[56] Bei den Navigationsdiensten zumindest jener Teil, der die Routenberechnung vornimmt; zur Frage, ob die zugrundeliegenden Kartendaten und das Abonnement von Updates dazu selbst auch dazugezählt werden, siehe im vorigen Absatz.

[57] Unten II.6.

*3. Schlüsselmoment*

Der Schlüsselmoment des derzeitigen Produkthaftungsregimes ist jener Zeitpunkt, in dem der Endhersteller das fertige Produkt in Verkehr bringt, womit seine Haftung für alles, was das Produkt und dessen Sicherheitsmerkmale danach verändert, im Wesentlichen entfällt.[58] Dies war in der Vergangenheit gerechtfertigt, solange es sich um klassische körperliche Gegenstände handelte, deren Sicherheit und Zuverlässigkeit nicht mehr beeinflusst werden konnte, sobald diese Produkte die Sphäre des Herstellers (physisch) verlassen hatten, weshalb es durchaus sinnvoll war, zu diesem Zeitpunkt eine Grenze zu ziehen.

Bei Produkten, die bereits jetzt laufend (insbesondere) online mit Updates versorgt werden, die entweder ohnehin vom ursprünglichen Hersteller stammen oder ihm zumindest zuzurechnen sind, behält dieser jedoch die tatsächliche Kontrolle über das Produkt und dessen Sicherheit, auch nachdem es das Werk physisch verlassen hat. Spätere Aktualisierungen können dabei die Sicherheitsmerkmale des Produkts verändern und es nach Installation dieser Updates fehlerhaft machen, selbst wenn die Produkte zuvor (also bis dahin) den Sicherheitserwartungen entsprochen hatten.

Aus diesem Grund muss die neue Richtlinie den Schlüsselmoment in Fällen, in denen solche Updates oder sogar Upgrades bereitgestellt werden, vom Zeitpunkt der ursprünglichen Auslieferung auf jenen Zeitpunkt danach verlagern, an dem der Hersteller die Bereitstellung solcher Modifikationen einstellt. Erst dann gibt er die ihm zumindest bis dahin zurechenbare Kontrolle über das Produkt und dessen Sicherheitsmerkmale auf.

Dies sieht Art. 11 Abs. 2 NPHRL als Ausnahme von der (dem bisherigen Art. 7 lit. b PHRL ansonsten entsprechenden) Einrede des Art. 11 Abs. 1 lit. c NPHRL vor:[59] Die dort weiterhin auf den Zeitpunkt des Inverkehrbringens „eingefrorene" Fehlerhaftigkeit wird sozusagen wieder aufgetaut (und entfällt damit), wenn und solange die Kontrolle des Herstellers[60] fortbesteht über verbundene Dienste, Software samt Updates oder Upgrades dazu (einschließlich unterbliebener, aber gebotener Aktualisierungen!), oder bei wesentlichen Änderungen des Produkts durch den in Anspruch Genommenen selbst oder mit seiner Genehmigung.

---

[58] Dies ergibt sich insbesondere aus Art. 7 lit. b PHRL, wonach der Hersteller nicht haftet, wenn er nachweisen kann, „dass unter Berücksichtigung der Umstände davon auszugehen ist, dass der Fehler, der den Schaden verursacht hat, nicht vorlag, als das Produkt von ihm in den Verkehr gebracht wurde, oder dass dieser Fehler später entstanden ist". Dieser Zeitpunkt ist aber auch etwa Auslöser der Verfallfrist des Art. 11 PHRL und maßgeblich für die Einschätzung der berechtigten Sicherheitserwartungen (Art. 6 Abs. 1 lit. c PHRL).

[59] Zum Wortlaut siehe unten Fn. 76.

[60] Diese wird definiert in Art. 4 Z. 5 NPHRL als zumindest Genehmigung (oder eigene Durchführung) von Einbauten von Komponenten, Verbindung mit Software, Bereitstellung von Updates oder Upgrades dazu, oder Änderungen des Produkts nach Auslieferung.

*4. Fehlerhaftigkeit*

Der Begriff des Fehlers bleibt in der neuen Richtlinie im Großen und Ganzen derselbe – die angemessenen Sicherheitserwartungen liefern weiterhin die entscheidenden Benchmarks dafür. Der neue Art. 7 NPHRL gibt nunmehr jedoch mit einer nicht abschließenden Liste genauere Hinweise darauf, welche Faktoren bei der Bewertung der Fehlerhaftigkeit zu berücksichtigen sind.[61] Ausdrücklich erwähnt werden nunmehr auch der Vollständigkeit halber (ohne legistischen Mehrwert) die „gemäß Unionsrecht oder nationalem Recht" vorgeschriebenen Sicherheitsstandards.[62]

Verbesserungen der Standards nach Inverkehrbringen ändern weiterhin nichts am auf diesen Zeitpunkt zu beziehenden Sicherheitsmaßstab (Art. 7 Abs. 3 NPHRL). Im Gegensatz zum bisherigen Art. 6 Abs. 2 PHRL wird aber auch betont, dass bereits zuvor (und nicht erst „später") in Verkehr gebrachte, „bessere" Produkte das streitgegenständliche nicht alleine deshalb fehlerhaft machen. Dies entspricht der bisherigen Sichtweise, gibt es doch schon jetzt Produkte mit unterschiedlichen Sicherheitsstandards, die (typischerweise auch an unterschiedlichen Preisen erkennbar) parallel auf den Markt gebracht werden, wie etwa Autos mit verschiedenen (teilweise aufpreispflichtigen) Sicherheitsfeatures.[63] Es sind also die Sicherheitserwartungen an das konkrete Produkt maßgeblich und nicht an ein generisches Produkt im weitesten Sinne.

*5. Haftpflichtige*

Wer haftet nach den Bestimmungen der neuen Richtlinie? Hier sind keine größeren Änderungen zu erwarten, sondern eher eine Aktualisierung der ursprünglichen Liste angesichts von zwischenzeitlichen Änderungen beim Vertrieb der Produkte, insbesondere seit Hinzukommen des Onlinehandels, den es 1985 natürlich noch nicht gab.

---

[61] Gem. Art. 7 Abs. 2 NPHRL sind bei der Beurteilung der angemessenen Sicherheitserwartungen „alle Umstände" zu berücksichtigen, einschließlich: „(a) der Aufmachung und der Merkmale des Produkts, einschließlich seiner Kennzeichnung, seines Designs, seiner technischen Merkmale, seiner Zusammensetzung und seiner Verpackung und der Anweisungen für Montage, Installation, Verwendung und Wartung; (b) der vernünftigerweise vorhersehbaren Nutzung des Produkts; (c) der Auswirkungen der Fähigkeit des Produkts, nach seinem Inverkehrbringen oder seiner Inbetriebnahme weiter zu lernen oder neue Funktionen zu erwerben, auf das Produkt; (d) der nach vernünftigem Ermessen vorhersehbaren Auswirkungen anderer Produkte auf das Produkt, bei denen davon ausgegangen werden kann, dass sie zusammen mit dem Produkt verwendet werden, unter anderem durch eine Verbindung mit dem Produkt; (e) des Zeitpunktes, zu dem das Produkt in Verkehr gebracht oder in Betrieb genommen wurde, oder, wenn der Hersteller nach diesem Zeitpunkt die Kontrolle über das Produkt behält, des Zeitpunktes, ab dem das Produkt nicht mehr unter Kontrolle des Herstellers steht; (f) der einschlägigen Sicherheitsanforderungen des Produkts einschließlich sicherheitsrelevanter Cybersicherheitsanforderungen; (g) Produktrückrufen oder sonstiger relevanter Eingriffe einer zuständigen Behörde oder eines in Art 8 genannten Wirtschaftsakteurs im Zusammenhang mit der Produktsicherheit; (h) der spezifischen Bedürfnisse der Gruppe von Nutzern, für die das Produkt bestimmt ist; (i) im Falle eines Produkts, dessen Zweck gerade darin besteht, Schäden zu verhindern, der Tatsache, dass das Produkt diesen Zweck nicht erfüllt."

[62] Vgl. *Koziol/Apathy/B.A. Koch*, Haftpflichtrecht III, 3. Aufl., Rn. B/166.

[63] Vgl. *Koziol/Apathy/B.A. Koch*, Haftpflichtrecht III, 3. Aufl., Rn. B/169, B/185.

*a) Die Haftpflichtigen in der derzeitigen Richtlinie*

Die derzeitige PHRL sieht ein Kaskadensystem der Haftung vor, das die Primärlast dem Hersteller des Endprodukts aufbürdet, die Haftung also auf ihn kanalisiert. An seiner Stelle haften alternativ diejenigen, die durch die Anbringung ihres Namens oder ihrer Marke auf den Produkten den Eindruck erwecken, selbst Produzent, ohne tatsächlich in die Herstellung involviert gewesen zu sein (Anscheins- oder Quasihersteller),[64] sowie jene, welche die in das Endprodukt eingebauten Bauteile oder die darin verarbeiteten Rohstoffe geliefert haben (wenn die Fehlerhaftigkeit des Endprodukts auf Mängel dieser Teile zurückzuführen ist, Art. 3 Abs. 1 PHRL).[65]

Können diese primär haftenden Personen nicht erreicht werden (insbesondere, wenn sie sich außerhalb der EU befinden), tritt die Person, die die Waren in den Binnenmarkt importiert, in die Fußstapfen des Herstellers, so dass die Geschädigten bei der Verfolgung ihrer Produkthaftungsansprüche z. B. die Vorteile der Brüssel-Ia-Regelung in Anspruch nehmen können (Art. 3 Abs. 2 PHRL).[66]

Bleiben die in dieser Liste bislang aufgeführten Personen unbekannt, tritt der Lieferant oder Händler des Produkts als Ersatzschuldner ein, es sei denn, er gibt die Identität seines Vormannes in der Lieferkette rechtzeitig bekannt (Art. 3 Abs. 3 PHRL).[67]

*b) Die Haftpflichtigen nach der künftigen Richtlinie*

Die neue Richtlinie ändert diese Liste durch Klarstellungen sowie durch Erweiterung des Kreises möglicher Haftpflichtiger etwas ab.

Zu beachten ist allerdings, dass – ebenso wie bisher[68] – auch die neue Regelung nur dann greift, wenn der Haftungsgrund in der Fehlerhaftigkeit des Produkts liegt. Art. 2 Abs. 4 lit. b NPHRL sagt dazu ausdrücklich, dass Ansprüche vom neuen Regime unberührt bleiben (und daher gesondert verfolgt werden können), „die eine geschädigte Person gemäß den nationalen Vorschriften über die vertragliche oder außervertragliche Haftung aus anderen Gründen als der Fehlerhaftigkeit eines Produkts gemäß dieser Richtlinie hat, einschließlich nationaler Vorschriften zur Durchführung von Unionsrecht". Alternative Haftungsgrundlagen wie eine verschuldensabhängige Haftung oder sogar die verschuldens*un*abhängige Haftung aufgrund anderer Risiken bleiben somit unberührt. Das Opfer eines fehlerhaften Autos kann daher z. B. alternativ auch den Fahrer (aus Verschulden) oder dessen Halter (aus EKHG) in Anspruch nehmen. Haftungsgrund ist im letzten Fall zwar nicht ein Verschulden, aber ein anderes Risiko als ein Produktfehler.

---

[64] *Koziol/Apathy/B.A. Koch*, Haftpflichtrecht III, 3. Aufl., Rn. B/51 ff. Vgl. jüngst EuGH, Urt. v. 7.7.2022 – Rs. C-264/21 (Keskinäinen Vakuutusyhtiö Fennia).

[65] *Koziol/Apathy/B.A. Koch*, Haftpflichtrecht III, 3. Aufl., Rn. B/39.

[66] *Koziol/Apathy/B.A. Koch*, Haftpflichtrecht III, 3. Aufl., Rn. B/58 ff.

[67] *Koziol/Apathy/B.A. Koch*, Haftpflichtrecht III, 3. Aufl., Rn. B/67 ff.

[68] Vgl. die folgenden drei EuGH Entsch.: Urt. v. 25.4.2002 – Rs. C-52/00 (Kommission/Frankreich) – Rn. 22; Urt. v. 25.4.2002 – Rs. C-154/00 (Kommission/Griechenland) – Rn. 18; Urt. v. 25.4. 2002 – Rs. C-183/00 (González Sánchez) – Rn. 31.

*aa) Primär Haftpflichtige*

Gemäß Art. 8 Abs. 1 NPHRL haftet – so wie bisher – in erster Linie der (End-)Hersteller des fehlerhaften Produktes (lit. a) oder der Hersteller eines darin verbauten Einzelteils oder Rohstoffs, der zur Fehlerhaftigkeit des Endproduktes beigetragen hat (lit. b).

Mit der Definition des „Herstellers" in Art. 4 Z. 10 NPHRL wird auch der Anscheinshersteller ausdrücklich hinzugezählt (lit. b), des Weiteren aber auch jemand, der das Produkt nicht für den Markt, sondern für den eigenen Gebrauch hergestellt hat (lit. c).[69] Letzteres mag nach der *Veedfald*-Entscheidung allerdings nicht weiter überraschen.[70]

Art. 8 Abs. 2 NPHRL stellt dem Hersteller haftungsrechtlich auch Personen gleich, die nach Inverkehrbringen des Produkts daran wesentliche Veränderungen[71] vornehmen und dann erneut in Vertrieb bringen. Zu denken ist dabei etwa an das Tuning von Kraftfahrzeugen als Beispiel.

*bb) Sekundär Haftpflichtige*

Weitere Ergänzungen der Liste der haftenden Personen in der neuen Richtlinie sind eher eine konsequente Weiterentwicklung als eine tatsächliche Änderung. Sofern kein Hersteller im obigen Sinne im Binnenmarkt ansässig ist, haftet wie bisher der von ihm zur Einfuhr des Produktes in den Binnenmarkt eingesetzte Importeur.

An dessen Stelle kann aber auch der so genannte „Bevollmächtigte" in Anspruch genommen werden (Art. 8 Abs. 1 lit. c sublit. ii NPHRL),[72] ein Akteur, den bereits frühere Rechtsakte wie die Marktüberwachungsverordnung[73] oder die Medizinprodukteverordnung[74] erfasst haben. Dabei handelt es sich gemäß Art. 4 Z. 11 NPHRL um jemanden, der „von einem Hersteller schriftlich beauftragt wurde, in seinem Na-

---

[69] Dies ergibt sich aus der Definition des „Herstellers" in Art. 4 Z. 10 lit. c NPHRL, wonach darunter auch eine Person fällt, die „ein Produkt für den Eigenbedarf entwickelt, herstellt oder produziert".

[70] EuGH, Urt. v. 10.5.2001 – Rs. C-203/99 (Veedfald).

[71] Diese sind in Art. 4 Z. 18 NPHRL definiert. Sofern nicht bereits kraft Gesetzes als wesentlich festgeschrieben, fallen darunter im Wesentlichen sicherheitsrelevante Umbauten und Veränderungen. Genannt sind ausdrücklich etwa „Änderungen der ursprünglichen Leistung, Verwendung oder Bauart des Produkts, ohne dass eine solche Änderung in der ursprünglichen Risikobewertung des Herstellers vorgesehen ist," oder „Änderungen der Gefährdungsart bzw. Änderungen, die neue Gefahren bergen oder das Ausmaß des Risikos erhöhen".

[72] Art. 4 Z. 11 NPHRL definiert den „Bevollmächtigten" als „jede in der Union ansässige natürliche oder juristische Person, die von einem Hersteller schriftlich beauftragt wurde, in seinem Namen bestimmte Aufgaben wahrzunehmen".

[73] Art. 3 Abs. 12 Verordnung (EU) 2019/1020 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über Marktüberwachung und die Konformität von Produkten sowie zur Änderung der Richtlinie 2004/42/EG und der Verordnungen (EG) Nr. 765/2008 und (EU) Nr. 305/2011, ABl. L 169/1 vom 25.6.2019.

[74] Art. 2 Abs. 32 Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung

men bestimmte Aufgaben wahrzunehmen". Handelt es sich dabei um den Importeur, haftet er bereits in dieser Eigenschaft, es sollen also bestimmte andere vom Hersteller als Repräsentanten namhaft gemachte Personen mit Sitz im Binnenmarkt angesprochen werden.

*cc) Tertiär Haftpflichtige*

Wenn keiner der beiden sekundär Haftpflichtigen in der EU ansässig ist, kann (erst) stattdessen der so genannte „*Fulfilment*-Dienstleister" auf Schadenersatz geklagt werden, ein weiterer Akteur, der bereits z. B. aus der Marktüberwachungsverordnung bekannt ist.[75] Darin spiegeln sich die Veränderungen im Warenvertrieb seit 1985 wider, auch im Hinblick auf körperliche Gegenstände. Heutzutage kaufen die Verbraucher Produkte direkt von einem z. B. Nicht-EU-Hersteller, der keinen eigentlichen Importeur mehr als Zwischenhändler in der EU hat, sondern stattdessen einen Logistikdienstleister[76] einsetzt, um den Verkauf in bestimmte Regionen wie die EU zu vereinfachen, ohne formal als Importeur der Waren aufzutreten (was zu einer Haftung in dieser Eigenschaft führen würde).

*dd) Quartär Haftpflichtige*

Der Verkäufer haftet nach wie vor, wenn alle Stricke reißen, also keine der bislang genannten Anspruchsgegner greifbar sind. Neu ist allerdings, dass auch bestimmte Online-Plattformen, wie sie aus dem Gesetz über digitale Dienste bekannt sind,[77] an seiner Stelle haften können, die nicht selbst als Händler auftreten, sofern die Voraussetzungen von Art. 6 Abs. 3 des Gesetzes über digitale Dienste erfüllt sind. Auch dies spiegelt die heutige Welt des Online-Verkaufs wider, in der Unternehmen wie Amazon es den Verbrauchern ermöglichen, Produkte nicht nur bei diesem Unternehmen selbst, sondern auch bei einigen Drittanbietern zu kaufen, die die Dienste von Amazon als Plattform in Anspruch nehmen, wo die eigentlichen (Kauf-)Vertragsparteien überhaupt erst zusammengebracht werden.

Die Haftung von Händler oder Online-Plattform entfällt, wenn sie „binnen eines Monats nach Eingang" der entsprechenden Anfrage[78] der geschädigten Person den

(EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates, ABl. L 117/1 vom 5.5.2017.

[75] Art. 3 Abs. 11 VO (EU) 2019/1020.

[76] Die Definition des „*Fulfilment*-Dienstleisters" in Art. 4 Z. 13 NPHRL verlangt, dass dieser mehr als nur eine der folgenden Dienstleistungen anbietet: „Lagerhaltung, Verpackung, Adressierung und Versand eines Produkts […]", wobei reine Versandleistungen alleine nicht erfasst werden.

[77] Art. 4 Z. 16 NPHRL verweist zur Definition der „Online-Plattform" ausdrücklich auf Art. 3 lit. i Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), ABl. L 277/1 vom 27.10.2022.

[78] Bislang sprach Art. 3 Abs. 3 PHRL lediglich von einer „angemessenen Zeit", ohne sie konkret zu bestimmen.

Vormann in der Lieferkette namhaft machen. Damit sind diejenigen, die die Produkte lediglich vertreiben, wie schon bisher nur „Ersatzbeklagte", sofern niemand aus den ersten drei Gruppen innerhalb der Union greifbar ist, während Letztere wie der Hersteller solidarisch mit diesem haften.

Sofern solcherart mehrere dieser in Art. 8 NPHRL aufgelisteten „Wirtschaftsakteure" haftbar sind, verweist Art. 14 NPHRL auf die nationalen Rechte für deren Rückgriffsansprüche untereinander.

### *6. Beweisprobleme*

Die PHRL aus 1985 enthält eine eher simpel gestrickte Bestimmung darüber, wer was beweisen muss – im Wesentlichen muss das Opfer alle Elemente des Anspruchs nachweisen, also seinen Schaden, die Fehlerhaftigkeit des Produkts sowie den Kausalzusammenhang zwischen beidem.[79] Die Tatsache, dass dies seit 1985 immer schwieriger geworden ist, wurde im fünften Kommissionsbericht 2018 anerkannt, in dem er dies als die „schwierigste Voraussetzung für eine Entschädigung" bezeichnete, insbesondere in Fällen von neuen digitalen Technologien.[80]

Die neue Richtlinie sieht hier erhebliche Änderungen vor, um diese Herausforderungen für die Geschädigten zumindest etwas zu entschärfen. Die NPHRL führt dabei sowohl Vorschriften über den Zugang zu Beweismitteln als auch über die Beweislast ein.

#### *a) Offenlegung von Beweismitteln (Art. 9 NPHRL)*

Art. 9 NPHRL verlangt im Wesentlichen, dass beide (!) Streitparteien entscheidungsrelevante Beweise vorlegen, die sich in ihrer jeweiligen ausschließlichen Verfügungsgewalt befinden, wenn auch nur im unbedingt notwendigen und verhältnismäßigen Maße (Abs. 3) und gekoppelt mit Vorkehrungen zum Schutz bestimmter Interessen, z. B. von Geschäftsgeheimnissen und anderen vertraulichen Informationen (Abs. 4 und 5). Welche Maßnahmen die Gerichte dabei treffen, bleibt nationalem Recht überlassen. Sie können allerdings dabei auch verlangen, dass die notwendigen Informationen, soweit zumutbar, „in leicht zugänglicher und leicht verständlicher Form" vorgelegt werden (Abs. 6).

Auf Klägerseite wird dazu in Abs. 1 vorausgesetzt, dass der geltend gemachte Anspruch zumindest ausreichend „plausibel" gemacht worden ist, bevor die Offenlegung von Beklagtenseite verlangt werden kann – damit wird sogenannten „*fishing expeditions*" von vornherein ein Riegel vorgeschoben. Beklagte können ihrerseits erst dann die Herausgabe verlangen, wenn sie ihren Bedarf daran zur Abwehr der Schadenersatzansprüche „ausreichend nachgewiesen" haben (Abs. 2).

---

[79] Art. 4 PHRL sagt dazu nur: „Der Geschädigte hat den Schaden, den Fehler und den ursächlichen Zusammenhang zwischen Fehler und Schaden zu beweisen."

[80] Fünfter Kommissionsbericht (Fn. 5), 5.

*b) Beweislast (Art. 10 NPHRL)*

Art. 10 NPHRL startet zwar im Wesentlichen mit einer ähnlichen Grundnorm wie bislang Art. 4 PHRL, verlangt also vom Kläger den Nachweis aller anspruchsbegründenden Elemente. Darauf folgen allerdings drei Ausnahmen, die ihm dabei entgegenkommen:

Die Fehlerhaftigkeit des Produktes wird in Abs. 2 (widerleglich, Abs. 5) vermutet, wenn die Beklagten ihrer in Art. 9 NPHRL ausgeführten Pflicht zur Offenlegung von Beweismitteln nicht nachgekommen sind, wenn dem Kläger zumindest der Nachweis gelungen ist, dass das Produkt gesatzte Regeln der Produktsicherheit nicht erfüllt, vor allem aber auch dann, wenn er wenigstens beweisen kann, „dass der Schaden durch eine offensichtliche Funktionsstörung des Produkts bei vernünftigerweise vorhersehbarer Verwendung oder unter normalen Umständen verursacht wurde" (Art. 10 Abs. 2 lit. c NPHRL).

Der Kausalzusammenhang zwischen einem bereits feststehenden Produktfehler und dem geltend gemachten Schaden wird gemäß Abs. 3 (ebenso widerleglich) vermutet, „wenn […] der entstandene Schaden von der dem betreffenden Fehler typischerweise entsprechenden Art ist".

Schließlich kann Fehlerhaftigkeit, Kausalzusammenhang oder beides (!) gemäß Abs. 4 vermutet werden, wenn nach Ausschöpfung der Möglichkeiten von Art. 9 NPHRL „und unter Berücksichtigung aller relevanten Umstände des Falles" es trotzdem „insbesondere aufgrund der technischen oder wissenschaftlichen Komplexität übermäßig schwierig ist", den Nachweis dafür zu erbringen, sofern (kumulativ!) der Kläger zumindest die Wahrscheinlichkeit von Fehler, Kausalität oder beidem nachweisen konnte (damit aber eben noch nicht das nötige Beweismaß erreichen konnte; die Vermutung füllt die Lücke zwischen erbrachtem und erforderlichen Beweis also gewissermaßen auf).

*7. Einreden*

Was die Einreden betrifft, so wurde der Katalog aus der geltenden PHRL und dessen Art. 7 im Wesentlichen kopiert und in die neue NPHRL eingefügt (natürlich mit einigen notwendigen Anpassungen). Leider wurde auch die lange umstrittene Einrede des Entwicklungsrisikos – bisher Art. 7 lit. e PHRL, jetzt Art. 11 Abs. 1 lit. e NPHRL – im Wesentlichen unverändert übernommen.[81]

Da sich der Schlüsselmoment der alten Haftungsregelung bei Aktualisierungen und Upgrades nun auf das Ende von deren Bereitstellung verlagert (oben II.3.), musste sich dies natürlich auch in der Liste der Einreden niederschlagen. Im Wesentlichen kann sich der Beklagte nicht darauf berufen, dass der Fehler wahrscheinlich noch

[81] Zur Kritik an der Einrede des Entwicklungsrisikos siehe nur *Fairgrieve et al.*, Product Liability Directive, in: Machnikowski (Hrsg.), European Product Liability: An Analysis of the State of the Art in the Era of New Technologies, 2016, 17 (77 ff.). Siehe auch den vierten Kommissionsbericht (Fn. 4), 8 f.; sowie die Stellungnahme des ELI zum Entwurf der NPHRL (Fn. 22), 21 f.

nicht vorhanden war, als das Produkt ursprünglich in Umlauf gebracht wurde, wenn und solange er danach tatsächlich noch die Kontrolle über das Produkt behalten hat.[82]

*8. Verjährung*

Auch die derzeitige Regelung der Verjährung (Art. 10 PHRL) bleibt im Wesentlichen mit Art. 16 NPHRL bestehen. Die (immer noch) dreijährige Verjährungsfrist beginnt ebenso weiterhin ab zumindest zumutbarer oder tatsächlicher Kenntnis der Geschädigten von Schaden, Fehlerhaftigkeit und der Person des Haftpflichtigen (was weiterhin auch Wissen um diese Eigenschaft als solche über die reine Identität hinaus voraussetzt). Damit ist in Österreich wie bisher auch nach künftigem Produkthaftungsrecht keine gesonderte gesatzte Produkthaftungs-Verjährungsregel erforderlich.

Die bisherige Präklusionsfrist von 10 Jahren in Art. 11 PHRL war immer schon ein Fremdkörper im Schadenersatzrecht und nicht nur aus diesem Grund abzulehnen.[83] Mit der Neuregelung in Art. 17 NPHRL scheint diese Regel zwar fortzubestehen, die Formulierung lässt es aber nunmehr zu, die Frist nicht als Präklusions-, sondern als Verjährungsfrist umzusetzen, womit der subjektiven Verjährungsfrist von Art. 16 PHRL eine „lange" objektive Verjährungsfrist an die Seite gestellt wird, die bereits mit Inverkehrbringen des Produktes startet und nicht erst mit Schädigung oder Kenntnis davon. Updates oder Upgrades führen hier – im Gegensatz zu Art. 10 Abs. 2 NPHRL bei den Einreden – zu keiner Verschiebung; lediglich bei „wesentlichen Veränderungen" am Produkt startet die Frist erst mit dem Vertrieb danach (Art. 17 Abs. 1 lit. b NPHRL).

Neu ist vor allem aber auch ein (offensichtlich eher zähneknirschendes) Zugeständnis des EU-Gesetzgebers an die Rechtsprechung des EGMR, der zufolge eine zehnjährige absolute Verjährungsfrist jedenfalls bei Körperverletzungen menschenrechtswidrig wäre. Daher wurde mit Art. 17 Abs. 2 NPHRL die zehnjährige objektive Frist wenigstens bei latenten Personenschäden auf 25 Jahre ausgedehnt, wenn die Geschädigten zuvor kein Verfahren einleiten konnten. Damit ist zwar der *Howald Moor*-Entscheidung des EMRK Rechnung getragen,[84] noch nicht jedoch seiner jüngsten Entscheidung in der Rs. *Jann-Zwicker*, die – zumindest in den dort gegenständlichen Asbestfällen – für den Beginn der (langen) Frist die Kenntnis des Schadens durch die Geschädigten vorauszusetzen scheint.[85]

---

[82] Art. 11 Abs. 2 NPHRL sieht vor: „Abweichend von Absatz 1 Buchstabe c wird ein Wirtschaftsakteur nicht von der Haftung befreit, wenn die Fehlerhaftigkeit des Produkts auf eine der folgenden Ursachen zurückzuführen ist, sofern sie der Kontrolle des Herstellers unterliegt: a) einen verbundenen Dienst, b) Software, einschließlich Software-Updates oder -Upgrades, c) das Fehlen von Software-Updates oder -Upgrades, die zur Aufrechterhaltung der Sicherheit erforderlich sind, d) eine wesentliche Änderung an dem Produkt."

[83] Vgl. *Koziol/Apathy/B.A. Koch*, Haftpflichtrecht III, 3. Aufl., Rn. B/253; *Fairgrieve et al.*, in: Machnikowski, European Product Liability, 17 (95 ff.).

[84] EGMR, Urt. v. 11.3.2014 – Rs. 52067/10 und 41072/11 (Howald Moor et al./Schweiz).

[85] EGMR, Urt. v. 13.2.2024 – Rs. 4976/20 (Jann-Zwicker und Jann/Schweiz).

## III. Ausblick

Die NPHRL wurde am 23.10.2024 nach Manuskriptabschluss verabschiedet und trat am 9.12.2024 in Kraft.[86] Die Mitgliedstaaten haben nunmehr zwei Jahre bis zum 9.12.2026 Zeit, um die neue Richtlinie in ihr jeweiliges nationales Deliktsrecht umzusetzen (Art. 22 Abs. 1 NPHRL).

Ein bisher nicht behandelter Aspekt wird in der neuen Richtlinie trotz zunehmender praktischer Relevanz leider gänzlich ausgeklammert: die Frage, wer für Schäden durch generalüberholte („*refurbished*") Produkte aufkommen soll, wenn diese sich erst nach der Überholung als fehlerhaft erweisen. Die betroffenen Produkte waren ja ursprünglich fabrikneu und haben als solche ihren Weg zu einem Erstnutzer gefunden. Nach einiger Zeit wird das nun von diesem bereits gebrauchte Produkt an den Aufbereiter weitergegeben, der es in einen wiederverkaufsfähigen Zustand versetzt und in der Regel beim neuerlichen Vertrieb behauptet, das generalüberholte Produkt sei wieder „so gut wie neu". Sobald es den zweiten Nutzer erreicht hat, stellt sich heraus, dass das Produkt defekt ist. Der Aufbereiter ist nicht jemand, der das ursprüngliche Produkt „wesentlich verändert" (wie in Art. 8 Abs. 2 NPHRL definiert), ganz im Gegenteil – das aufgearbeitete Produkt wird in den Zustand zurückversetzt, in dem es sich bei seinem ersten Inverkehrbringen befunden hat, und der Verbraucher erwartet, dass es genauso sicher ist wie zu diesem Zeitpunkt in der Vergangenheit.

Lässt man den Beitrag des Erstnutzers außer Acht (er haftet ohnehin nicht im Rahmen der PHRL), so gibt es immer noch (zumindest) zwei mögliche Beklagte – den Aufbereiter und den ursprünglichen Hersteller. Der Fehler kann in einer dieser beiden Sphären entstanden sein. Man könnte den Aufbereiter in erster Linie als (neuen) Hersteller haftbar machen (was mit dem Konzept der Anscheinshersteller und der wesentlichen Veränderer vereinbar ist), dem Aufbereiter aber gestatten, den ursprünglichen Hersteller in Regress zu nehmen, wenn der Fehler dem Produkt bereits von Anfang an innegewohnt hatte (das heißt schon zu einem Zeitpunkt, als es erstmals in Verkehr gebracht wurde). Der ursprüngliche Hersteller würde damit gegenüber demjenigen, der sein Produkt generalüberholt, wie dessen Zulieferer behandelt werden.

Trotz dieses Versäumnisses ist die NPHRL aber unzweifelhaft ein großer Schritt nach vorn, der eindeutig zu begrüßen ist.

---

[86] Richtlinie (EU) 2024/2853 des Europäischen Parlaments und des Rates vom 10.10.2024 über die Haftung für fehlerhafte Produkte und zur Aufhebung der Richtlinie 85/374/EWG des Rates, ABl. L 2024/2853 vom 18.11.2024.

# Digitalisierung und Immaterialgüterrecht

## Spotify, Netflix und Amazon Prime Video … rechtlich betrachtet[1]

*Manfred Büchele*



## I. Medienkonvergenz – Streaming

Wie werden Medien heutzutage konsumiert? Nun, der Wunsch, die Inhalte physisch in Besitz zu nehmen, tritt zurück und wird ersetzt durch die bloße Nutzung, durch den reinen Genuss der Inhalte, ergänzt um das aktive Teilen und Diskutieren derselben. Willkommen in der Welt des multimedialen Internet, denn ebendort ist das Streaming gerade dabei, eine entscheidende Hürde zu nehmen, indem es dem linearen Konsum von Medieninhalten (Radio, Fernsehen) langsam aber sicher den Rang abläuft.

Früher war das anders: Für gewöhnlich standen Radio und Fernseher im Wohnzimmer, und die eigene Betätigung beschränkte sich darauf, zwischen mehr oder weniger vielen (Kabel- bzw. Satelliten-)Sendern hin und her zu schalten – Mission abgeschlossen. Sendungen begannen zu einem festgelegten Zeitpunkt. Wer zu spät oder ohne Aufzeichnungsgerät kam, den bestrafte das Leben. Die Alternativen bestanden darin, auf Wiederholungen zu vertrauen oder ins Konzert respektive ins Kino zu gehen.

---

[1] Erweiterte und mit Fußnoten versehene schriftliche Fassung eines am 13.5.2024 im Rahmen der Ringvorlesung „Internationalisierung und Digitalisierung – Internationalisierung des Rechts im digitalen Zeitalter" gemeinsam mit *Christian Handig* gehaltenen Vortrags.

Dann kam die Digitalisierung und mit ihr die CD und die DVD, robust und mit hoher Speicherkapazität ausgestattet. Mit ihnen änderte sich auch die Art der Inhalte, weil mit der vermehrten Verfügbarkeit von Serien das Murmeltier bald täglich grüßte: Statt sich Woche für Woche mit nur einer Folge zu einem bestimmten Zeitpunkt zufrieden geben zu müssen, konnte man mehrere Folgen, ganze Staffeln, mehr oder weniger zeitunabhängig am Stück ansehen – das Binge-Watching war geboren.

Mit dem Aufkommen des Internet änderte sich die Mediennutzung erneut: Download- und On-demand-Dienste gewannen an Bedeutung, dank mobiler Endgeräte konnten die Medieninhalte auch ortsunabhängig genutzt werden. Etwa zur gleichen Zeit begannen Fernsehsender und Rundfunkanstalten ihre Inhalte online in Mediatheken anzubieten. Mit der zunehmenden Verbreitung von Breitband-Internetverbindungen wurden zudem Online-Recorder populärer, mit denen Audio- und Videoinhalte in der Cloud aufgezeichnet werden konnten.

Mit *Spotify*, *Netflix*, *Amazon Prime Video* und all den anderen Streamingdiensten wurde es für breite Bevölkerungsschichten alltäglich, geradezu selbstverständlich, jederzeit und überall hören und sehen zu können, wonach einem gerade der Sinn steht.[2] Man hat schließlich die Wahl, wann, wo und wie man die Inhalte konsumiert. Auf dem Smartphone, am Laptop oder am Fernseher? – Alles kein Problem! Wann läuft welcher Film oder welche Serie? All das ist inzwischen nachrangig. Mit dem Voranschreiten der Technik gewann auch der eigene Komfort.

Heutzutage betten Online-Plattformen wie *YouTube* die von ihnen angebotenen Social Media-, Streaming- und Cloudfunktionen direkt in ihre Dienste ein. Mit Fug und Recht kann der legendäre Zeitgeist somit eine Konvergenz des Medienangebots und der Mediennutzung für sich beanspruchen, in der sich fortschreitende Entwicklungen der Technologie, gesellschaftliche Veränderungen und der Einfluss neuer Plattformen widerspiegeln. Insofern ist es nur konsequent, dass die Vielfalt des Angebots und die Flexibilität im Konsum die heutige Medienlandschaft prägen.

Mittlerweile ist allerdings eine gewisse Trendumkehr zu erkennen. Die Auswahl an Medieninhalten und Anbietern ist inzwischen unüberschaubar groß geworden, mitunter braucht es allein aus diesem Grund einen gewissen Mut zur Lücke. Darüber hinaus ist der Streaming-Markt stärker segmentiert als je zuvor. Das befeuert die Nachfrage nach „Alternativen". So hatte die Onlinepiraterie im Jahr 2021 einen Tiefpunkt erreicht, seither nimmt sie wieder zu.[3] Im Detail: Im Jahr 2017 lag die Anzahl der Zugriffe auf unrechtmäßig im Internet angebotene Inhalte bei etwa elf pro Internetnutzer pro Monat. Anfang 2021 waren fünf Zugriffe zu verzeichnen, wohingegen es Ende 2022 schon wieder sieben waren – Tendenz steigend. Ein interessantes Detail am Rande zu der von den Nutzern verwendeten Zugriffsmethode: 58 % der

[2] Manche Formate werden nach wie vor gerne live mitverfolgt, wie z. B. der Song Contest oder Sportereignisse.

[3] Siehe *EUIPO*, Online Copyright Infringement in the European Union 2023, 30, abrufbar unter https://www.euipo.europa.eu/en/publications/online-copyright-infringement-in-eu-2023 (Abrufdatum: 16.7.2024).

„raubkopierten" Inhalte wurden gestreamt, während auf 32 % per Download zugegriffen wurde.[4]

Die Gründe für das Wiederaufleben der Onlinepiraterie sind vielfältig. Wie schon erwähnt ist das Angebot auf zahlreiche Plattformen verstreut. Das damit einhergehende Werben um die Gunst der Konsumenten ist lediglich imstande, Anteile auf einem gesättigten Markt zu verschieben, was wiederum die Kosten für alle Beteiligten in die Höhe treibt (Stichwort Inflation). Zudem sind viele Inhalte als Stream gar nicht verfügbar. Und *last but not least* hat das Streamingzeitalter an einem altbekannten Problem der Branche, dass nämlich die einzelnen Anbieter nur über inhaltlich, territorial und/oder zeitlich zersplitterte Lizenzrechte verfügen, wenig geändert.

Ein neues Phänomen ist allerdings hinzugekommen: Im Unterschied zu klassischen physischen Medien „besitzt" man beim Streaming nichts mehr. Man hat vielfach keine Handhabe dagegen, dass die Plattformen ihr Angebot laufend umsortieren und sich Titel nur vorübergehend in den Onlinekatalogen finden. Für all das gibt es sogar einen Fachbegriff: *Streaming anxiety* – die Angst, Inhalte aus dem Online-Abonnement nicht dauerhaft behalten zu können. Diese *„Streamingangst"* lässt die Absätze von physischen Speichermedien seit einigen Jahren wieder steigen. Sie könnte aber sogar einer der Gründe sein, weshalb die Onlinepiraterie in Form von Downloads schon vorhandener „raubkopierter" Inhalte wieder zunimmt.[5]

Ein Blick in die Nutzungsbedingungen zweier bedeutender Streaminganbieter lässt erkennen, dass die *„Streamingangst"* nicht ganz unbegründet ist:

- Bei *Netflix* können sich die verfügbaren Inhalte je nach Region unterscheiden; die Nutzer müssen damit rechnen, dass sich die Inhalte von Zeit zu Zeit ändern.[6] Zudem sind nicht alle Serien und Filme als Download verfügbar. Wird das Konto gekündigt, werden sämtliche Downloads gelöscht. Im Übrigen laufen Downloads nach einer gewissen Zeit jedenfalls ab.[7] Die Unsicherheit der Nutzer wird verstärkt, indem aus *Netflix* entfernte Titel auch nicht mehr als Download zur Verfügung stehen.
- *Amazon Prime Video* behält sich das Recht vor, digitale Inhalte nach Ablauf des Nutzungszeitraums automatisch vom Gerät des Nutzers zu entfernen. „Gekaufte" digitale Inhalte stehen grundsätzlich weiterhin zum Herunterladen oder Streamen

---

[4] *EUIPO*, Online Copyright Infringement in the European Union 2023, 9, abrufbar unter https://www.euipo.europa.eu/en/publications/online-copyright-infringement-in-eu-2023 (Abrufdatum: 16.7.2024).

[5] Der Durchschnittsnutzer kann die von den Streamingdiensten eingesetzten Systeme für das Digital Rights Management (DRM), insbesondere *PlayReady* und *Widevine*, nicht umgehen und keine Streams dauerhaft speichern.

[6] *Netflix*, Nutzungsbedingungen, Abschnitt 4.3., abrufbar unter https://help.netflix.com/de/legal/termsofuse (Abrufdatum: 16.7.2024).

[7] *Netflix*, Herunterladen von Titeln zum Offline-Ansehen, abrufbar unter https://help.netflix.com/de/node/54816 (Abrufdatum: 16.7.2024).

zur Verfügung, sind jedoch aufgrund von möglichen Lizenzbeschränkungen des Inhalteanbieters oder aus anderen Gründen eventuell nicht mehr verfügbar.[8]

Im englischsprachigen Raum würde man im Zusammenhang mit der Nutzungsform des Streaming von einer „*Disruption*" sprechen, einem Vorgang, in dem eine Innovation ein bestehendes Geschäftsmodell ablöst. Im gegebenen Zusammenhang hat das Aufkommen von Streamingdiensten zweifellos an den traditionellen Modellen der Mediennutzung gerüttelt. Das Streaming ermöglicht es den Nutzern, die Inhalte orts- und zeitunabhängig direkt über das Internet abzurufen. Dieser Wandel ist nicht nur als Tatsache an sich schon bedeutend, sondern zudem „disruptiv" in dem Sinn, dass er weitreichende Auswirkungen auf die Art und Weise hat, wie Inhalte erstellt, vertrieben und konsumiert werden.

## II. Streaming – technische Aspekte

Unter „Streaming" versteht man die kontinuierliche Online-Übertragung von digitalen Medieninhalten wie z. B. Audio- oder Videodateien. Im Unterschied zum herkömmlichen Download müssen die Daten beim Streaming nicht vollständig heruntergeladen werden, ehe sie abgespielt werden können. Stattdessen werden die Daten schubweise übertragen und zwischengespeichert, was eine schnelle Wiedergabe der Inhalte ermöglicht.[9] Die zwischengespeicherten Daten werden von den nachfolgenden Daten überschrieben; eine aus technischer Sicht „vollständige" Audio- oder Videodatei entsteht auf dem Wiedergabegerät somit nie.

Beim „Live-Streaming" werden die Medieninhalte (nahezu) in Echtzeit übertragen. Im Gegensatz zu vorher aufgezeichneten oder gespeicherten Dateien erfolgt ein Live-Stream in dem Moment, in dem das Ereignis stattfindet. Das können beispielsweise Live-Übertragungen von Veranstaltungen, Konzerten, Sportereignissen, Interviews oder anderen Ereignissen sein. Das entscheidende Merkmal eines Live-Streams ist allerdings sein linearer Charakter. Die Hörer/Seher können hier nur entscheiden, ob sie die live gestreamten Inhalte konsumieren möchten oder nicht. Den Beginn, den Ablauf und/oder den Inhalt des Streams können sie nicht beeinflussen, zumal der Streaminganbieter die Hoheit über das Geschehen hat. *Dazn*, *Twitch* und *YouTube Live* sind namhafte Dienste, die das Live-Streaming anbieten.

Mit „Streaming on demand" können Videos, Musik usw. jederzeit auf Abruf konsumiert werden. Die Nutzer entscheiden hier selbst, welche Inhalte an welchem Ort und zu welcher Zeit sie sehen oder hören möchten. Im Unterschied zu Live-Streams,

[8] *Amazon Prime Video*, Nutzungsbedingungen Punkt 4. h. Eingeschränkte Lizenz für Digitale Inhalte und Punkt 4. i. Verfügbarkeit von Gekauften Digitalen Inhalten, abrufbar unter https://www.primevideo.com/-/de/help/ref=atv_hp_nd_nav?language=de_DE&nodeId=G202095490 (Abrufdatum: 16.7.2024).

[9] Siehe *Pabst*, in: Handig/Hofmarcher/Kucsko (Hrsg.), urheber.recht, 3. Aufl., 2023, § 41a UrhG Rn. 21 f.

bei denen die Inhalte in Echtzeit übertragen werden, gibt es beim Streaming on demand keine festgelegten Sendezeiten. *Spotify*, *Netflix* und *Amazon Prime Video* sind nur einige jener Dienste, die das Streaming on demand anbieten und die Nutzer davon „befreien", die Inhalte vor ihrem Konsum erst herunterladen zu müssen.

## III. Streaming – urheberrechtliche Aspekte

Vom Streaming können verschiedene Werkarten i. S. d. Urheberrechts betroffen sein.[10] Die wichtigsten sind:

- Lieder/Songs und Musikalben sind als Werke der Tonkunst urheberrechtlich geschützt.[11] Sie stehen auf Streamingdiensten wie z. B. *Spotify*, *Deezer*, *Apple Music* usw. zum Abruf zur Verfügung.
- Filme, Serien, Videos und Fernsehsendungen erfahren Schutz als Werke der Filmkunst.[12] Sie werden von Streamingdiensten wie *Netflix*, *Amazon Prime Video*, *Disney+*, *Sky*, *Dazn*, *YouTube* usw. online angeboten.
- Für Video- und Computerspiele kommt der Schutz als Computerprogramm bzw. Filmwerk in Betracht.[13] Sie können über Dienste wie beispielsweise *Twitch* oder *YouTube Live* gestreamt werden.
- Auch Bücher können gestreamt werden, und zwar als Hörbuch. Sie und i. d. R. auch Podcasts sind als Sprachwerke urheberrechtlich geschützt.[14] Ihr Abruf ist über *Audible*, *Spotify* usw. möglich.

Die Streaminganbieter benötigen für den Upload und das Übertragen bzw. Zugänglichmachen der Inhalte entsprechende Lizenzen. Je nach Art des Streaming sind unterschiedliche Verwertungsrechte betroffen, insbesondere aber das Vervielfältigungs-, das Sende- und das Zurverfügungstellungsrecht.

### *1. Vervielfältigungsrecht*

Vervielfältigen ist das Festhalten eines Werks zur wiederholbaren Wiedergabe gegenüber den menschlichen Sinnen, und zwar egal in welchem Verfahren, in welcher Menge und ob vorübergehend oder dauerhaft.[15] Als besonders breit angelegtes Verwertungsrecht umfasst das Vervielfältigungsrecht sowohl das erstmalige Festlegen als auch das Reproduzieren bzw. Kopieren eines bereits vorhandenen Werkstücks. Auf das verwendete Speichermedium und die dabei eingesetzte Technik kommt es

---

[10] Die sogenannten verwandten Schutzrechte nach den §§ 66 ff. öUrhG bleiben hier außer Betracht.

[11] Vgl. § 1 Abs. 1 öUrhG.

[12] Vgl. § 4 öUrhG.

[13] Vgl. § 2 Z. 1 und § 4 öUrhG.

[14] Vgl. § 2 Z. 1 öUrhG.

[15] Vgl. § 15 Abs. 1 öUrhG.

nicht an, sodass das Vervielfältigen auch die digitale Speicherung sowie den Up- und Download von Inhalten umfasst.[16]

Es liegt auf der Hand, dass die Streaminganbieter eine Vervielfältigung vornehmen, weil die Streams an sich schon eine Werkkopie bei den Anbietern voraussetzen. Der Abruf der Streams durch die Nutzer berührt das Vervielfältigungsrecht ebenfalls, ungeachtet dessen, dass die im Cache gespeicherten Daten von den nachfolgenden überschrieben werden. Die zwischengespeicherten Daten sind allerdings i. d. R. vorübergehende Vervielfältigungen,[17] die ohne gesonderte Zustimmung der Rechteinhaber zulässig sind.[18]

Die Regelung zu den vorübergehenden Vervielfältigungen privilegiert – aus Sicht der Nutzer – sowohl das Live-Streaming als auch das Streaming on demand, sofern die Streams von einer rechtmäßigen Vorlage ausgehen.[19] Und mit besonderem Augenmerk auf das Streaming on demand: Eine zeitlich versetzte, asynchrone Wiedergabe in der Form, dass die Nutzer den Wahrnehmungsvorgang zwischenzeitlich unterbrechen oder beliebig wiederholen können, ändert m. E. nichts daran, dass die Zwischenspeicherungen aus Nutzersicht keine eigenständige wirtschaftliche Bedeutung haben.[20]

### *2. Senderecht*

Dem Urheber ist das ausschließliche Recht vorbehalten, sein Werk drahtlos oder mit Hilfe von Leitungen zu senden und dadurch der Öffentlichkeit wahrnehmbar zu machen.[21] Mit anderen Worten: Der Urheber bestimmt über das aktive Senden, nicht aber über das passive Empfangen von Sendungen. Kennzeichnendes Merkmal einer Sendung ist daher auch, dass die Empfänger den Beginn, den Ablauf und/oder den Inhalt der Übertragung nicht beeinflussen können.[22]

Beim Live-Streaming (gerade von Radio- oder Fernsehprogrammen) können die Hörer/Seher nur entscheiden, ob sie die gestreamten Inhalte konsumieren möchten

---

[16] Siehe *Büchele*, Urheberrecht, 3. Aufl., 2023, 44.

[17] Nach § 41a öUrhG ist eine vorübergehende Vervielfältigung zulässig,

1. wenn sie flüchtig oder begleitend ist und
2. wenn sie ein integraler und wesentlicher Teil eines technischen Verfahrens ist und
3. wenn ihr alleiniger Zweck die Übertragung in einem Netz zwischen Dritten durch einen Vermittler oder eine rechtmäßige Nutzung ist und
4. wenn sie keine eigenständige wirtschaftliche Bedeutung hat.

[18] Siehe *Mitterer*, Rechteerwerb beim grenzüberschreitenden Streaming, ipCompetence 2014/12, 56 (58).

[19] Greifen die Nutzer „freiwillig und in Kenntnis der Sachlage", sprich wissentlich, auf illegale Streaming-Quellen zu, ist die Ausnahme für vorübergehende Vervielfältigungen nicht anwendbar, weil sich die Nutzer nicht auf ihre Unkenntnis berufen können. Siehe dazu ausf. EuGH, Urt. v. 26.4.2017 – Rs. C-527/15 (Stichting Brein) ÖBl-LS 2017, 238 (*Handig*) = MR-Int 2017, 33 (*Walter*) = ecolex 2017, 790 (*Zemann*) = jusIT 2017, 94 (*Staudegger*).

[20] A. A. *Pabst*, in: Handig/Hofmarcher/Kucsko, urheber.recht, 3. Aufl., 2023, § 41a UrhG Rn. 38.

[21] Vgl. § 17 öUrhG.

[22] Siehe *Büchele*, Urheberrecht, 3. Aufl., 48.

oder nicht. Aufgrund seines linearen Charakters berührt das Live-Streaming das Senderecht.[23]

### *3. Zurverfügungstellungsrecht*

Das Zurverfügungstellungsrecht behält dem Urheber das Anbieten von Werken zum interaktiven Abruf vor. Gemeint ist damit ein Werkzugriff, den Mitglieder der Öffentlichkeit nach freier Wahl – sowohl hinsichtlich des Orts wie auch der Zeit, drahtgebunden oder drahtlos – vornehmen können; die Nutzer entscheiden, wann und wo sie die (Online-)Inhalte wahrnehmen wollen.[24] Davon abgesehen muss das Zurverfügungstellen für eine Mehrzahl von Personen bestimmt sein, die zahlenmäßig nicht bestimmt abgegrenzt und nicht durch wechselseitige Beziehungen oder durch Beziehungen zum Anbieter der Inhalte persönlich miteinander verbunden sind.[25]

Da die Nutzer beim Streaming on demand den Beginn und auch sonst den Ablauf der von ihnen ausgewählten Streams beeinflussen können, ist das Streaming on demand als öffentliches Zurverfügungstellen zu qualifizieren. Die Inhalte müssen nur für den interaktiven Abruf öffentlich bereitgehalten werden; dass die Nutzer die Streams tatsächlich abrufen, ist für das Zurverfügungstellen nicht vonnöten.

## IV. Sonderfall Online-Recorder

Online-Recorder ermöglichen die Aufzeichnung von Sendungsinhalten in der Cloud, wobei als Gegenstand der Aufzeichnung neben Fernsehprogrammen auch Radiosendungen usw. in Betracht kommen. Für die technische Umsetzung stehen verschiedene Verfahren zur Auswahl, heutzutage ist aber das sogenannte Deduplizierungsverfahren üblich. Dabei wird von einer Sendung eine Masterkopie erstellt, die die Nutzer später (online) streamen können. Die Besonderheit des Deduplizierungsverfahrens liegt darin, dass die Masterkopie für jeden Zugriff lediglich „referenziert" wird, ohne dass ein weiteres Dateiduplikat für jeden einzelnen Nutzer entstehen würde.[26]

Beim Deduplizierungsverfahren ist die vom Diensteanbieter angelegte Masterkopie von zentraler Bedeutung. Diese dient als Kopiervorlage und wird (zumeist) auch dann erstellt, wenn kein Nutzerauftrag vorliegt.[27] Die auf dem Deduplizie-

---

[23] Siehe *Mitterer*, ipCompetence 2014/12, 56 (59).

[24] Vgl. § 18a öUrhG.

[25] Siehe *Büchele*, Urheberrecht, 3. Aufl., 52.

[26] Siehe *Büchele/Strasser*, Online-Recorder. Ein Blick in die urheberrechtliche Zukunft, ÖBl 2023, 51 (51).

[27] Vgl. OGH 22.9.2020, 4 Ob 149/20w (OTT-Dienste) MR 2020, 307 (*Korn/Walter*) = jusIT 2021, 28 (*Schmitt*) = ÖBl 2021, 86 (*Handig*): „erfolgt doch die Speicherung […] initiativ durch die Beklagte auf ihren Servern" und OGH 26.11.2020, 4 Ob 185/20i (OTT-Dienste II) MR 2021, 80 (*Walter*) = ÖBl 2021, 280 (*Büchele*): „Auch wenn kein einziger Kunde einen individuellen Auftrag […] erteilt"; zur Abhängigkeit vom Nutzerauftrag siehe hingegen EuGH, Urt. v. 13.7.2023 – Rs. C-426/21 (Oci-

rungsverfahren aufbauende sogenannte Replay-Funktion nimmt in diesem Zusammenhang eine besondere Rolle ein, als sie es den Nutzern erlaubt, Sendungen zumeist bis zu sieben Tage lang im Nachhinein abzurufen. Wird die Funktion aktiviert, entstehen Aufzeichnungen selbst dann, wenn kein einziger individueller Aufnahmewunsch vorliegt.[28]

Es ist nicht zu übersehen, dass sowohl die Aufnahme- als auch die Replay-Funktion einen Mehrwert generieren, weil die Nutzer nicht mehr an den ursprünglichen Ausstrahlungszeitpunkt gebunden sind. Dabei fällt insbesondere ins Gewicht, dass ein Online-Recorder die Masterkopie für eine Vielzahl weiterer Nutzer zum Abruf bereithält. Folgerichtig kommt dem Anbieter eines Online-Recorders die Organisationshoheit über den gesamten Ablauf zu und er nimmt insoweit eine zentrale Rolle im Vervielfältigungsgeschehen ein. Die sogenannte *Privatkopieausnahme*[29] kann er in diesem Fall nicht für sich in Anspruch nehmen.[30]

Das Zurverfügungstellungsrecht verletzen Online-Recorder ebenfalls, weil sie an die Öffentlichkeit gerichtete Wiedergabehandlungen vornehmen. Ihr Streamingangebot spricht zweifelsohne ein zahlenmäßig unbestimmtes Publikum sowie recht viele Personen an. Davon abgesehen erfolgt die von Online-Recordern ermöglichte Wiedergabe in einem anderen technischen Verfahren als die ursprüngliche „Erstsendung" – Online-Recorder streamen die Signale ja über das Internet an die Nutzer.[31]

## V. Geoblocking

Lizenzen an urheberrechtlich geschützten Werken werden i. d. R. nur eingeschränkt eingeräumt.[32] Die Begrenzungen können sich auf bestimmte Inhalte, bestimmte Verwertungsrechte, auf gewisse Zeiträume oder auf bestimmte geografische Bereiche oder Sprachen beziehen. Erhält der Lizenznehmer lediglich eine räumlich einge-

---

lion IPTV Technologies) ÖBl 2024, 39 (*Büchele/Strasser*) = MR 2023, 220 (*Walter*) = ecolex 2023, 1060 (*Hofmarcher*): „geht die Initiative für jede Aufnahme in der Praxis grundsätzlich vom Endnutzer aus, der die Online-Aufnahmefunktion selbst aktiviert und den aufzuzeichnenden Inhalt auswählt. Sobald ein Programm von einem ersten Nutzer ausgewählt worden ist, wird die Aufnahme jedem anderen Nutzer zur Verfügung gestellt, der den aufgezeichneten Inhalt ansehen möchte."

[28] Siehe *Büchele/Strasser*, ÖBl 2023, 51 (51 f.).

[29] Vgl. Art. 5 Abs. 2 lit. b Info-RL (Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABl. L 167/10 vom 22.6.2001).

[30] EuGH, Urt. v. 29.11.2017 – Rs. C-265/16 (VCAST) ÖBl-LS 2018, 27 (*Handig*) = MR-Int 2017, 113 (*Fischer*) = ecolex 2018, 164 (*Albrecht*); EuGH, Urt. v. 13.7.2023 – Rs. C-426/21 (Ocilion IPTV Technologies) ÖBl 2024, 39 (*Büchele/Strasser*) = MR 2023, 220 (*Walter*) = ecolex 2023, 1060 (*Hofmarcher*).

[31] EuGH, Urt. v. 29.11.2017 – Rs. C-265/16 (VCAST) ÖBl-LS 2018, 27 (*Handig*) = MR-Int 2017, 113 (*Fischer*) = ecolex 2018, 164 (*Albrecht*); *Büchele/Strasser*, ÖBl 2023, 51 (55 f.).

[32] Die RL 2014/26/EU enthält besondere Vorschriften für die grenzüberschreitende Vergabe von Online-Rechten an Musik. Im Vordergrund steht die Förderung von Mehrgebietslizenzen und – damit einhergehend – das Entstehen gesamteuropäischer Musikdienste.

schränkte Lizenz, muss er sicherstellen, dass die betreffenden Inhalte nur im entsprechenden Gebiet konsumiert, nur dort abgerufen werden können.

Das Problem besteht darin, dass das Internet, das *World Wide Web*, seiner Konzeption nach keine geografischen Grenzen kennt, weshalb online verfügbare Inhalte grundsätzlich weltweit abrufbar sind. Mit dem Geoblocking schränken die Lizenznehmer die weltweite Abrufbarkeit ein: Innerhalb des Lizenzgebiets erhalten die Nutzer Zugriff auf die Inhalte, außerhalb werden sie blockiert – und zwar je nach geografischem Standort, der über die IP-Adresse ermittelt wird.[33]

Das Geoblocking ermöglicht Zensur sowie Zugangs- und Preisdiskriminierung bei Waren und Dienstleistungen, mit seiner Hilfe kann aber auch das Online-Glücksspiel in seine nationalen Schranken verwiesen werden.[34] Im Folgenden liegt das Hauptaugenmerk allerdings auf etwas anderem, nämlich dem Zugang zu urheberrechtlich geschützten Inhalten im Ausland. Genauer: Wie und unter welchen Voraussetzungen können die Musik, die Serien und Filme aus den entsprechenden Abonnements auch länderübergreifend genutzt werden, so etwa im Urlaub, wenn das Geoblocking dem Konsum entgegensteht?

Seit April 2018 ermöglicht die Verordnung zur grenzüberschreitenden Portabilität von Online-Inhaltediensten im Binnenmarkt (kurz: Portabilitätsverordnung) genau das. Sie folgt insofern dem Trend zur ortsunabhängigen Mediennutzung und erlaubt Abonnenten, während eines vorübergehenden Aufenthalts in einem anderen EU-Mitgliedstaat (nicht aber z. B. in Großbritannien oder der Schweiz) auf im Wohnsitzmitgliedstaat entgeltlich bereitgestellte[35] Online-Inhalte zuzugreifen. Dazu fingiert die Portabilitätsverordnung, dass der Zugriff aus einem anderen Mitgliedstaat als aus dem eigenen Wohnsitzmitgliedstaat erfolgt gilt.[36] Mit anderen Worten: Trotz vorübergehender grenzüberschreitender Bereitstellung des Dienstes werden die Verwertungshandlungen als im Wohnsitzstaat getätigt angesehen.

Den Nutzern dürfen für die Portabilität keine Mehrkosten entstehen und die Streaminganbieter müssen den gleichen Funktionsumfang zu den gleichen Bedin-

---

[33] IP-Adressen werden lokal bzw. regional vergeben/zugewiesen. Dadurch verfügen sie über eine nationale „Abstammung", die sie einem bestimmten Land zuordenbar macht.

[34] Um dennoch auf die gewünschten (aber blockierten) Inhalte zugreifen zu können, greifen Nutzer auf ein Virtual Private Network (VPN) oder einen Proxy-Server zurück. Der Zugriff erfolgt dabei über einen Vermittler, der keinen gesperrten IP-Adressbereich verwendet, wodurch der „echte" Standort des Nutzers dem Zielrechner gegenüber verborgen bleibt.

[35] Art. 3 Abs. 1 Portabilitätsverordnung spricht von einem „Online-Inhaltedienst, der gegen Zahlung eines Geldbetrags bereitgestellt wird".

[36] Vgl. Art. 4 Portabilitätsverordnung. Die Streaminganbieter können zusätzlich die Inhalte des vorübergehend aufgesuchten Mitgliedstaats anbieten; sie müssen das aber nicht tun. Art. 7 Portabilitätsverordnung bestimmt, dass Vertragsklauseln, die die grenzüberschreitende Portabilität beschränken oder verbieten, nicht durchsetzbar sind (Vorrang der Portabilitätsverordnung vor vertraglichen Absprachen). Das Recht eines Drittstaats für anwendbar zu erklären, gilt als Umgehung und ist ebenfalls unzulässig (zwingende Anwendung der Portabilitätsverordnung unabhängig von einer entgegenstehenden Rechtswahl).

gungen wie im Wohnsitzmitgliedstaat gewährleisten.[37] Befolgen die Diensteanbieter diese verpflichtenden Vorgaben nicht, richten sich die Rechtsfolgen nach nationalem Recht; die Portabilitätsverordnung selbst sieht diesbezüglich keine ausdrücklichen Sanktionen vor.

Abseits der Regeln der Portabilitätsverordnung darf das Geoblocking weiterhin eingesetzt werden. Außerdem: Der allgemeine grenzüberschreitende EU-weite Zugriff im Onlinehandel (E-Commerce) gehört nicht zum Regelungsgegenstand der Portabilitätsverordnung. Wird also das Geoblocking eingesetzt, um den Zugriff auf einen ausländischen Onlineshop zu verhindern oder die Zahlung zu verweigern, oder erfolgt eine Umleitung auf eine andere Länderversion des Shops, ist nicht die Portabilitätsverordnung, sondern die sogenannte Geoblockingverordnung[38] einschlägig.

Um den weiteren Ausführungen besser folgen zu können, sollen an dieser Stelle einige wichtige Tatbestandselemente der Portabilitätsverordnung näher erläutert werden.

Art. 2 Z. 1 Portabilitätsverordnung definiert den Begriff des „Abonnenten". Dabei handelt es sich um einen Verbraucher, der auf Grundlage eines Vertrags mit einem Anbieter über die Bereitstellung eines Online-Dienstes berechtigt ist, im Wohnsitzstaat auf den Dienst zuzugreifen und ihn zu nutzen.

Nach Art. 2 Z. 2 Portabilitätsverordnung sind „Verbraucher" natürliche Personen, die einen Vertrag mit einem Diensteanbieter nicht für Zwecke ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit abschließen. Damit sind auch Geschäftsreisende in ihrer Eigenschaft als Verbraucher erfasst, nicht hingegen Unternehmen als solche, die ihr „gewerbliches" Streamingabonnement folgerichtig nicht ihren Mitarbeitern im Ausland zur Verfügung stellen können.

Der von Art. 2 Z. 3 Portabilitätsverordnung legaldefinierte „Wohnsitzmitgliedstaat" bezeichnet den tatsächlichen und dauerhaften Wohnsitz des Abonnenten in einem EU-Mitgliedstaat.[39] Demgegenüber erfasst der „vorübergehende Aufenthalt in einem Mitgliedstaat" nach Art. 2 Z. 4 Portabilitätsverordnung den zeitlich begrenzten Aufenthalt in einem anderen Mitgliedstaat als dem Wohnsitzmitgliedstaat. Urlaube, (Geschäfts-)Reisen oder Lern- bzw. Studienaufenthalte zwecks „Lernmobilität" sind jedenfalls vorübergehend,[40] im Übrigen fehlt eine nähere zeitliche Präzisierung. Dieser Umstand bringt vordringlich die Diensteanbieter in die Bredouille: Sie stehen vor dem Problem, zum einen ihren Kunden gegenüber die Portabilität ihrer

[37] ErwGr. 19 und 21 Portabilitätsverordnung.

[38] Verordnung (EU) 2018/302 des Europäischen Parlaments und des Rates vom 28. Februar 2018 über Maßnahmen gegen ungerechtfertigtes Geoblocking und andere Formen der Diskriminierung aufgrund der Staatsangehörigkeit, des Wohnsitzes oder des Ortes der Niederlassung des Kunden innerhalb des Binnenmarkts und zur Änderung der Verordnungen (EG) Nr. 2006/2004 und (EU) 2017/2394 sowie der Richtlinie 2009/22/EG, ABl. L 60 I/1 vom 2.3.2018.

[39] Die Bestimmung eines einzigen Wohnsitzes beugt Missbräuchen vor, weil ansonsten das Preisgefälle innerhalb der EU dazu führen würde, dass die Nutzer ständig von einem anderen Mitgliedstaat aus auf die Inhalte zugriffen.

[40] ErwGr. 1 Portabilitätsverordnung.

Inhalte nicht im erforderlichen Umfang zu gewährleisten. Zum anderen könnten sie aber auch die Rechteinhaber benachteiligen, falls sie den vorübergehenden Charakter zu großzügig auslegen. Mangels weiterer Anhaltspunkte ist ein „vorübergehender Aufenthalt" in einem anderen Mitgliedstaat m. E. ein jeder Aufenthalt, der nicht auf Dauer angelegt ist und entsprechend zu keiner Verlagerung des Wohnsitzes in einen anderen Mitgliedstaat führt.[41]

Die Praxis wählt einen pragmatischen Blickwinkel und schlägt folgende Lösungsansätze vor:

– *Netflix* erläutert in seinen Nutzungsbedingungen, dass man auf die entsprechenden Inhalte hauptsächlich in dem Land zugreifen kann, in dem man das Konto erstellt hat, und außerdem nur in den geografischen Regionen, in denen die jeweiligen Inhalte lizensiert sind.[42] Für „Zweitwohnsitze oder häufige Reisen an denselben Ort" schlägt *Netflix* folgendes Prozedere vor:[43]

„Stellen Sie einmal pro Monat am Hauptort, an dem Sie Netflix nutzen, über Ihr Mobilgerät eine Verbindung zum Internet her, öffnen Sie die Netflix-App oder rufen Sie in einem Webbrowser Netflix.com auf und streamen Sie für ein paar Sekunden einen Titel, um eine Verbindung zu Netflix herzustellen. Führen Sie dann die gleichen Schritte an Ihrem Zielort durch, um Netflix unterbrechungsfrei zu nutzen."

– *Sky* schränkt den Zeitraum für den vorübergehenden Aufenthalt auf 37 Tage ein. Nach 30 Tagen erfolgt eine Benachrichtigung, dass innerhalb von sieben Tagen von zuhause aus auf *Sky* zugegriffen werden muss, um zu bestätigen, dass sich der Wohnsitz weiterhin in Österreich befindet.[44]

Nach Art. 2 Z. 5 Portabilitätsverordnung erbringen „Online-Inhaltedienste" Dienstleistungen für ihre Abonnenten in deren Wohnsitzmitgliedstaat.[45] Hier geht es hauptsächlich um Dienste, deren Hauptzweck das Bereitstellen von audiovisuellen, visuellen oder akustischen Medien in linearer oder nicht linearer Form ist. Erfasst sind sowohl das Live-Streaming als auch das Streaming on demand von Musik, Filmen, Bildern, E-Books, Spielen usw., aber auch Konzerte oder Sportveranstaltungen. Die Bereitstellung der Dienste muss über das Internet (online) erfolgen, portabel sein und im Wohnsitzmitgliedstaat erbracht werden.[46] Zu diesen Diensteanbietern zählen z. B. Musik-Streamingdienste wie *Spotify* oder *Deezer* oder Video-Plattformen wie *Netflix*

---

[41] So auch *Heyde*, Die Portabilitätsverordnung. Auswirkungen auf die Lizenzverträge, ZUM 2017, 712 (718 f.).

[42] *Netflix*, Nutzungsbedingungen, Abschnitt 4.3., abrufbar unter https://help.netflix.com/de/legal/termsofuse (Abrufdatum: 16.7.2024).

[43] *Netflix*, Netflix außerhalb Ihrer Adresse verwenden, abrufbar unter https://help.netflix.com/de/node/24853 (Abrufdatum: 16.7.2024).

[44] *Sky*, Nutzung von Sky im EU-Ausland, abrufbar unter https://sky.at/hilfe/s/article/nutzung-von-sky-im-eu-ausland (Abrufdatum: 16.7.2024).

[45] Online-Inhaltedienste, die ihre Leistungen kostenlos (ohne Zahlung eines Geldbetrags) bereitstellen, können sich der Portabilitätsverordnung freiwillig unterwerfen (sogenanntes *Opt-In* gemäß Art. 6 Portabilitätsverordnung).

[46] Die Anbieter der Dienste müssen ihren Sitz nicht innerhalb der EU haben.

oder *Amazon Prime Video*, aber auch der auf das Live-Streaming von Sportereignissen spezialisierte Anbieter *Dazn* oder Mischformen daraus wie *Sky* oder Gamingplattformen wie beispielsweise *Steam*.

Art. 2 Z. 6 Portabilitätsverordnung erläutert, wann ein Dienst als „portabel" gilt. Kann ein Abonnent auf einen Dienst zugreifen und ihn nutzen, ohne auf einen bestimmten Standort beschränkt zu sein, liegt die Portabilität vor, so z. B. bei Diensten, die online auf Laptops, Tablets oder Smartphones usw. abrufbar sind.[47]

## VI. Umgehung von Geoblocking

Der Anwendungsbereich der Portabilitätsverordnung ist relativ schmal. Den Heimataccount für einen vorübergehenden Aufenthalt ins EU-Ausland „mitzunehmen" beseitigt nicht sämtliche Schwierigkeiten, mit denen sich die Abonnenten von Streamingdiensten konfrontiert sehen. Erblicken die Nutzer ihr „Problem" beispielsweise in einer für sie nachteiligen Preisdifferenzierung, somit einer Preisgestaltung, die für ihr Heimatland vergleichsweise höhere Preise ausweist, oder ist in ihrem Heimatland – wiederum im direkten Vergleich ein- und desselben Anbieters – nur eine eingeschränkte Anzahl von Musik- oder Filmtiteln verfügbar, könnte das Umgehen von Geoblockingmaßnahmen durchaus Sinn ergeben.

Viele Streaminganbieter untersagen Umgehungshandlungen in ihren Nutzungsbedingungen oder legen fest, dass keine Techniken verwendet werden dürfen, um den eigenen Standort zu verschleiern:

- *Amazon Prime Video* bestimmt den geografischen Aufenthaltsort mittels entsprechender Technologien. Der jeweilige Aufenthaltsort darf durch keinerlei Technologien oder technische Methoden verdeckt oder verschleiert werden. Außerdem dürfen Systeme zum Schutz digitaler Rechte oder andere Schutzsysteme, die als Teil des Services verwendet werden, nicht deaktiviert, umgangen, verändert, außer Betrieb gesetzt oder anderweitig unterlaufen werden.[48]
- Nutzern von *Spotify* ist es untersagt, jedwede von *Spotify* genutzte Technologie sowie territoriale Beschränkungen zu umgehen.[49]

Wird eine Umgehung vorgenommen, droht mitunter die Beendigung des Streamingangebots durch den Diensteanbieter, ohne dass bereits bezahlte Abonnementgebühren rückerstattet würden.

---

[47] Vgl. ErwGr. 2 Portabilitätsverordnung.

[48] *Amazon Prime Video*, Nutzungsbedingungen Punkt 3. Geografische Unterschiede und Punkt 4. k. Allgemeine Einschränkungen (iv), abrufbar unter https://www.primevideo.com/help/ref=atv_hp_nd_nav?language=de_DE&nodeId=G202095490 (Abrufdatum: 16.7.2024).

[49] *Spotify*, Allgemeine Nutzungsbedingungen von Spotify, Nutzerrichtlinie Punkt 7.5. und 7.7., abrufbar unter https://www.spotify.com/at/legal/end-user-agreement/#7-nutzerrichtlinien (Abrufdatum: 16.7.2024).

- *Amazon Prime Video* kann den Zugang zum eigenen Service einschließlich aller als Teil des Services verfügbaren Abonnements jederzeit im eigenen Ermessen beenden. In diesem Fall erstattet *Amazon* die Abonnementgebühr anteilsmäßig zurück. Wird jedoch gegen die Nutzungsbedingungen verstoßen, erlöschen die Rechte automatisch. *Amazon* kann in diesem Fall den Zugriff auf den Service und auf digitale Inhalte im eigenen Ermessen ohne Rückerstattung von Gebühren mit sofortiger Wirkung widerrufen.[50]
- *Spotify* kann den Vertrag jederzeit kündigen und den Zugang jederzeit aussetzen, wie z. B. bei einer tatsächlichen oder vermuteten unautorisierten Nutzung des *Spotify*-Dienstes und/oder der Inhalte von *Spotify*, bei einer Nichteinhaltung der Vereinbarung. *Spotify* erstattet keine Beträge zurück, sofern dies im gesetzlichen Rahmen zulässig ist.[51]
- *Netflix* verfährt differenzierter: Wird *Netflix* über ein Virtual Private Network (VPN) genutzt, erscheint entweder der Fehlercode E106 oder es werden nur Serien und Filme gezeigt, für die *Netflix* die weltweiten Rechte besitzt. Bei einem werbefinanzierten Abo ist die Nutzung von *Netflix* über eine VPN-Verbindung nicht gestattet. Live-Veranstaltungen auf *Netflix* können generell nicht über ein VPN wiedergegeben werden.[52]

Ob eine Umgehung des Geoblocking eine technische Schutzmaßnahme gemäß § 90c Abs. 1 öUrhG verletzt, ist gesondert zu beurteilen. Um als technische Maßnahme zu gelten, muss die Maßnahme wirksam das Begehen von Urheberrechtsverletzungen verhindern oder einschränken.[53] In seinem Bestreben, den Zugriff aus außerhalb des Lizenzgebiets liegenden Ländern zu verhindern, kann man dem Geoblocking nicht absprechen, (auch) die durch ein unrechtmäßiges Zugänglichmachen ausgelösten Urheberrechtsverletzungen unterbinden zu wollen. Mit Blick auf die Wirksamkeit sind hier jene technischen Maßnahmen angesprochen, welche die Nutzung eines geschützten Inhalts durch eine Zugangskontrolle oder einen Schutzmechanismus wie Verschlüsselung oder einen Mechanismus zur Kontrolle der Vervielfältigung regeln.[54] Dessen ungeachtet sind die sanktionierten Umgehungshandlungen gedank-

[50] *Amazon Prime Video*, Nutzungsbedingungen 6. a. Kündigung, abrufbar unter https://www.primevideo.com/help/ref=atv_hp_nd_nav?language=de_DE&nodeId=G202095490 (Abrufdatum: 16.7.2024).

[51] *Spotify*, Allgemeine Nutzungsbedingungen von Spotify, Laufzeit und Kündigung Punkt 12., abrufbar unter https://www.spotify.com/at/legal/end-user-agreement/#7-nutzerrichtlinien (Abrufdatum: 16.7.2024).

[52] *Netflix*, Serien und Filme über ein VPN ansehen, abrufbar unter https://help.netflix.com/de/node/114701 und https://help.netflix.com/de/node/277 (Abrufdatum: 16.7.2024).

[53] Der rechtliche Schutz der Technik erfüllt als Vehikel die Aufgabe, mittelbar der Absicherung urheberrechtlicher Befugnisse zu dienen. Siehe *Büchele*, in: Ciresa (Hrsg.), Österreichisches Urheberrecht, 23. Aufl., 2023, § 90c UrhG Rn. 2.

[54] Vgl. § 90c Abs. 2 öUrhG sowie Art. 6 Abs. 3 Satz 2 Info-RL (Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABl. L 167/10 vom 22.6.2001).

lich von den Schutzmaßnahmen zu trennen. Da beim Vortäuschen einer regionsspezifischen IP-Adresse keine technische Schutzmaßnahme im Rechtssinn „umgangen" wird, liegt keine Umgehungshandlung i. S. d. § 90c öUrhG vor, die sanktioniert werden könnte.[55]

[55] *Büchele*, in: Ciresa, Urheberrecht, 23. Aufl., 2023, § 90c UrhG Rn. 22 m. w. N.

# Potential and Limitations of the Right to Data Portability Eight Years after the Adoption of the GDPR

*Stefano Troiano*



## I. Introduction

Data portability has undergone a rapid and impetuous evolution in European legislation during the last years. From being the content of a data subject's right to personal data, provided for by Art. 20 of the EU General Data Protection Regulation (GDPR), portability is increasingly becoming a commonly used concept even beyond the specific field of personal data, i. e., in the general data regulation framework, where it does not necessarily present itself as the object of a precise subjective right. Moreover, data portability is receiving specific consideration in certain areas from which it was initially excluded or in respect of which there is a need for more detailed regulation, such as health data[1] or consumer protection.[2] Therefore, it appears increasingly

[1] See EU Commission Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, Strasbourg, 3.5.2022, COM(2022) 197 final, 2022/0140 (COD) and, in particular, the first Section of Chapter II, devoted to the rights of natural persons in relation to the primary use of their personal electronic health data.

[2] The right to portability also appeared in European directives that modernised consumer protection in the digital market, in particular in Directive (EU) 2019/770 of the European Parliament

as a multifaceted and versatile concept, which can take on variable functions and contents. For this reason, some authors prefer to decline the concept in the plural today, speaking of 'portabilities', thus outlining the existence of different forms of portability in the EU legislation.[3]

The main driver of this transformation is easy to identify. Portability, as intimately connected to data circulation, is increasingly attractive, both from the perspective of the empowerment of data subjects and for its dynamic connotation as a tool enhancing data exchange and, ultimately, promoting the development of the digital economy and the opening of new data markets.

However, this growing consideration in the law is not matched by an adequate knowledge of the instrument in the practice, especially if the analysis focuses on the right to data portability under Art. 20 of the GDPR.

A recent survey on German users' knowledge of GDPR rights[4] showed that data portability is the data subject's right, among those provided for by the GDPR, that is known by the lowest percentage of respondents.[5] The number of judicial cases concerning the right to data portability in the Member States is also very low and no decision of the European Court of Justice can be mentioned on the matter so far.

Presumably, these difficulties arise from a plurality of factors, like, for example: the complexity of the legal situation set out in Art. 20 of the GDPR, which already includes a plurality of distinct aspects from the outset; its relative novelty, which makes it difficult to compare it with already known situations; the incompleteness of its regulation, which raises uncertainty; its uncertain practical feasibility because of the unavailability of technologies.

It is time, therefore, to take stock of the existing situation and verify the actual and unexpressed potential of data portability as an instrument, comparing it with its increasing new usecases. To examine the new dimensions of portability arising in the European scenario, reference will be made to the contribution by *Stefano Gatti* (see below), to which the present paper is ideally linked. In the present contribution, the

---

and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJEU L 136/1, 22.5.2019 and in Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, OJEU L 328/7, 18.12.2019 (so-called *omnibus*) in the rules on distance and off-premises contracts, when the contract relates to digital content or services and the consumer exercises the right of withdrawal. See below *Gatti*, in this volume.

[3] See *Gatti*, Dalla portabilità alle „portabilità": l'evolutione al plurale di un diritto (e concetto) chiave nella disciplina europea dei dati, European Journal of Private Law and Technology 2024, Iss. 1, 158.

[4] *Kuebler-Wachendorff et al.*, The Right to Data Portability: conception, status quo, and future directions, Informatik Spektrum 2021, Vol. 44, 264 (266 et seqq.).

[5] Approx. 30 % have heard of the right of data portability; this compared to almost 90 % who have heard of the right to erasure. The right of data portability is, at least among those who know it, the right whose content is least easy to grasp: on a scale of 2 to 5, the level of understanding is slightly above 2 (see *Kuebler-Wachendorff et al.*, Informatik Spektrum 2021, Vol. 44, 264 [266 et seqq.]).

focus will rather be on the critical analysis of the state of the art as regards the portability right of the GDPR eight years after its introduction and six years after its first application in practice in 2018. To begin with, it is appropriate to recall, albeit in summary, the essential features of the right to portability as outlined by the GDPR.

## II. The RtDP's Features Under the GDPR

As is well known, the right to data portability outlined by the GDPR (hereinafter: RtDP) is indeed a unitary right but with complex content, which may include up to three claims that are abstractly distinguishable from each other.[6] In particular, the RtDP includes (Art. 20 GDPR): 1) the right, under certain conditions, 'to receive from the controller the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used, and machine-readable format'; 2) the right 'to transmit those data to another controller without hindrance from the controller to whom the personal data have been provided';[7] 3) as well as, finally, again at his or her request, the right to have personal data transmitted directly from one controller to another, 'where technically feasible.'

The right to data portability is, moreover, a right whose exercise is subject to several general and specific conditions (Art. 20 para. 1 GDPR). If the data subject wants to request portability, it is first necessary that the processing involves personal data of the data subject, which he or she has provided to a controller. Secondly, the processing must be based on the data subject's consent pursuant to lit. a of Art. 6 para. 1 or lit. a of Art. 9 para. 2 GDPR or on a contract pursuant to lit. b of Art. 6 para. 1 GDPR. Finally, for data portability to be applicable the processing must be carried out by automated means.

## III. The RtDP's Novelty: Between Myth and Reality

The right to the portability of personal data, in the forms in which it is outlined in Art. 20 of the GDPR, has been counted by some early commentators as one of the most significant innovations introduced by the uniform European data protection

---

[6] *Somaini*, The right to data portability and user control: ambitions and limitations, Rivista di diritto dei media 2018, Iss. 3, 164 (165), speaks of a threefold content. According to *Pezza*, in: Riccio/Scorza/Belisario (eds.), GDPR e normativa privacy. Commentario, 2018, Art. 13 GDPR 203, however who speaks of a right with dual content. The latter author, therefore, does not consider the claim of the data subject to the direct transfer from one operator to another as a separate claim.

[7] For example, the right to portability allows a streaming music service user to transfer his or her playlists or music preferences from one streaming service to another at no additional cost.

framework. It has thus been referred to as 'a disruptive right'[8], a 'brand new right'[9], a 'major update of data regulation'.[10]

However, while it cannot be denied that this is a legal situation that was not present as such in the pre-existing regulatory framework, a more careful reading leads to downsizing the innovative charge of the provision in Art. 20, both because the right to portability has already appeared in fields of legislation other than that of personal data protection and because the distinctive features of the right to portability show non-negligible elements of continuity with other legal situations aimed to the protection of personal data already existing before the GDPR came into force.

Outside personal data protection, the instrument of data portability has a significant antecedent in the right to telephone number portability, which has been recognised for some years now to users of telephone services and which allows them to keep their telephone number when changing operator.[11]

If one then looks beyond the Italian borders and observes the international situation, both within and beyond the boundaries of the European Union, one can see that the target of endowing users with a broad right to portability can be found, for instance, in projects or experiments[12] already attempted in some European countries in

---

[8] *Kühling/Martini*, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht? EuZW 2016, Vol. 27 Iss. 12, 448 (450).

[9] *Scudiero*, Bringing Your Data Everywhere: A Legal Reading Of The Right To Portability, European Data Protection Law Review 2017, Vol. 3 Iss. 1, 119.

[10] *Wong/Henderson*, The right to data portability in practice: exploring the implications of the technologically neutral GDPR, International Data Privacy Law 2019, Vol. 9 Iss. 3, 173 (173 et seqq.).

[11] See Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), OJEU L 108/51, 24.4.2002.

[12] Briefly described by *Catalano*, Il diritto alla portabilità dei dati tra interessi individuali e prospettiva concorrenziale, Europa e diritto privato 2019, Iss. 3, 833 (837 et seqq.). In particular, the right to data portability finds its roots in the initiative launched in 2007 by a group of engineers in Chicago and known as the *Bill of Rights for Users of the Social Media,* a non-binding document aimed at codifying the fundamental rights of Internet users and the related duties of *website providers* (see *Smarr/Canter/Scoble/Arrington*, A Bill of Rights for Users of the Social Web, September 2007). In that context, the idea of portability was born as a tool to give users back full control of their data and thus make it as easy as possible for them to migrate their personal data from one platform to another, with the indirect pro-competitive effect of forcing Internet operators to compete with each other to make better products, to meet the needs of users and render them better ready to select among different alternatives in the market. This initiative gave rise to Google's *Data Takeout* tool in 2011 and then, as of 2018, to the *Data Transfer Project,* an open-source platform aimed at promoting the universal portability of data through full interoperability, even allowing the direct transfer of data from one operator to another at the user's request and without the need, in this case, for the double step of download and subsequent upload (the platform is joined, among others, by *Google* itself and other major Internet players like Twitter/X). See also *Pezza*, in: Riccio/Scorza/Belisario, GDPR, 2018, Art. 13 GDPR 202.

more or less recent times[13] as well as in similar initiatives undertaken overseas, specifically in the United States.[14]

Within the European Union, the regulation of a right to personal data portability has also been the subject of a recommendation by the European Data Protection Supervisor, who highlighted its usefulness as a tool for enhancing the rights of the data subject,[15] with the specific aim of enabling individuals to 'easily and freely change provider and transfer their personal data to another service provider'[16]. Other preparatory acts have also moved in the same direction.[17] Moreover, the right to portability was already provided for in Art. 18 of the Commission's GDPR Proposal, COM(2012) 11 final, albeit only in its basic version (right to receive data and to transmit them to a new data controller).

## IV. RtDP and Right to Access: A Comparison

As regards the relationship with the rights already attributed to the data subject by the former rules on personal data, the RtDP can be considered, for some of its features, as an evolution of the pre-existing right to access, from which it is now formally kept distinct in the regulatory framework of the Regulation.[18]

Although at one time (i. e. in the European Parliament Legislative Resolution of 12 March 2014) portability was recharacterised as an adjunct to the right to access, the debate in the Council soon brought the two rights back to their current separation. In the Council's Position 6/2016, the two rights already appear in separate articles, i. e. Art. 15 and 20. Compared to the Commission's wording, the legal basis is no longer limited to the transmission of the data, but also covers the descending phase of the receipt of the data by the original holder; the additional limitations in para. 3 and 4 also appear. Finally, the Commission's role in specifying technical standards in

---

[13] For instance, the Personal Health Recording developed by the Dutch Patent Association, the UK's 'MyData' Programme, or the French 'Mes Infos' project.

[14] Reference is made here to the actions known as 'Blue Button' and 'Green Button' in the health and energy fields, respectively.

[15] A function that the European Data Protection Supervisor understood to be closely linked to that of the introduction of a new right to be forgotten.

[16] See Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – 'A comprehensive approach on personal data protection in the European Union', OJEU C 181/1, 22.6.2011, 19.

[17] In particular, the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, Brussels, 4.11.2010, COM(2010) 609 final, and the European Parliament Resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union, 2011/2025(INI).

[18] This is underlined, among others, by *Ricci*, I diritti dell'interessato, in: Finocchiaro (ed.), Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali, 2017, 179 (229 et seq.).

relation to the format in which the data subject is entitled to receive the data disappears, nor is there any more reference to the formats that must be accepted by the receiving data controller.

Compared to the right to access under Art. 15 of the GDPR, the RtDP shows some similarities. In its minimum manifestation, the RtDP also allows, like the right to access, to acquire knowledge of the personal data that are stored and processed by the data controller, thus enabling the data subject to verify the scope and lawfulness of the processing.

From the right to access the RtDP, however, differs insofar as it allows, firstly, to obtain a personal copy of the data, that is to obtain the transfer of the data onto one's own personal medium (for the purposes of mere storage or for further personal use that does not involve other data transfers), and, secondly, insofar as it allows its holder to obtain not just any personal copy of the data in question, but a copy in a format that has certain characteristics, i. e. that must be structured, commonly used, and machine-readable:[19] these requirements, in short, allow a quick and easy re-use of the data for the purposes decided by the data subject. As already mentioned, the complexity of its content implies, as a further point of distinction from the right to access, that the RtDP also includes, albeit only as a possible object, the right to transfer the data to another data controller without hindrance, with the possibility, where technically feasible,[20] also of a direct transfer from one to the other.[21]

If, therefore, the right of access has an essentially 'static dimension', responding to the need to guarantee to the data subject only knowledge of the data being processed, the right to portability is concerned with regulating the 'dynamic dimension' of the data subject's control over the data being processed, projecting protection into the sphere of the availability of the data by the data subject himself or herself. In other words, the RtDP makes, or at least should make, its holder full and effective 'dominus' of the data concerning him or her, giving him or her the possibility not only to regain possession of them but also to reuse them according to his or her preferences, even by transferring them to third parties.

## V. The Two-Fold Rationale Underlying the RtDP

In the light of the latter remarks, the emergence of the RtDP could thus appear to be one of the fundamental stages in the process of progressive autonomisation of the

[19] On the other hand, the exercise of the right of access does not bind the data controller to comply with a particular format.

[20] The concept of 'technical feasibility' is not, however, precisely defined in the European regulation.

[21] A further difference from the right of access is the fact that the right to data portability only applies where processing is carried out on the basis of consent or where processing is necessary for the performance of a contract to which the data subject is party (see also below).

right to the protection of personal data as a legal situation distinct from the right to confidentiality (or privacy). By enhancing the data subject's power of control over the data to the highest level, the RtDP would indeed represent the fullest expression of the right to the protection of personal data in its positive projection, as opposed to the mere negative freedom not to be subjected to external interference in one's sphere of intimacy (right to privacy).

Seen in this perspective, the right to data portability is in line with the approach on which the system of personal data protection has traditionally been built ever since Directive 95/46/EC, as an instrument of maximum enhancement of data control[22] and thus as a fundamental right of the data subject[23] on a par with the other rights of which it is an evolution, starting with the right to access.[24] This is the perspective taken up, in the first instance, also by recital 68 of the GDPR, which expressly refers to the need to strengthen the data subject's power of control over his or her personal data.[25] It is therefore the primary expression of the right to informational self-determination, finding its basis in the guarantee enshrined in Art. 8 of the Charter of Fundamental Rights of the European Union (which, however, does not expressly mention the right to portability, whereas it specifically refers, in the context of personal data protection, to the right to access).

This perspective, by limiting itself to highlighting the functional continuity of the new instrument with respect to the pre-existing ones, does not, however, adequately take the implications into account arising from the choice of enhancing data control also in its more purely dynamic projection,[26] i. e. in terms of reuse of personal data in the direction of free circulation.

This opening up entails a radical transformation of the instrument, that, from the purely quantitative sphere (as a means of enhancing the extension and effectiveness of the control), goes directly to the qualitative level, affecting the very function of the instrument.

---

[22] See *Monteleone*, Il diritto alla portabilità dei dati. Tra diritti della personalità e diritti del mercato, LUISS Law Review 2017, Iss. 2, 202 (205). See also *Fenwick/Fertik/Jurcys/Minssen*, Data Portability Revisited: Toward the Human-Centric, AI-Driven Data Ecosystems of Tomorrow, Common Market Law Review 2024 (preprint version consulted at https://ssrn.com/abstract=4475106 [last accessed on: 1 September 2024]).

[23] On the RtDP as a fundamental right see *Pelino*, I diritti dell'interessato, in: Bolognini/Pelino/Astolfi (eds.), Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali, 2016, 171 (250) and *Somaini*, Rivista di diritto dei media 2018, Iss. 3, 164 (171).

[24] From this perspective, the RtDP is in line with other measures that similarly empower data subjects to manage or control the use of their personal data, such as the rights to information, access, rectification and erasure of personal data. See *Pezza*, in: Riccio/Scorza/Belisario, GDPR, 2018, Art. 13 GDPR 202.

[25] 'To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller.'

[26] *Battelli/D'Ippolito*, Il diritto alla portabilità dei dati personali, in: Tosi (ed.), Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice della Privacy, 2019, 185 (193).

This transformation can be seen on two levels: In the first place, allowing and indeed promoting, the re-use of data by the data subject and its transfer to new data controllers imply a logic of commodification of data as the object of enjoyment and exploitation by the data subject, for purposes that can be indifferently of a personal or economic nature. This reinforces, therefore, an economic and commodified conception of personal data,[27] which obscures their primary function as moments of expression of the individual's personality. Secondly, the purpose of facilitating data transfer, by encouraging the adoption by companies of tools favouring the interoperability of IT platforms, highlights the functionality of the provision also in the direction, distinguishable from the personalistic one, of the protection of individuals' personal data, of regulating the data market.[28]

It is from the joint analysis of these profiles that one can grasp the true – and from this unquestionable angle – innovative scope of the new instrument. The novelty lies precisely in the intrinsic multi-functionality[29] of this instrument that, due to its hybrid and complex quality or even ambiguity, ultimately represents the litmus test for the new delicate balance that the GDPR strikes between the protection of individual rights and the protection of the market.[30]

## VI. In a Nutshell: An Ambivalent Right

As we have seen, depending on how and for what purpose it is exercised by the data subject, the RtDP represents the highest expression of control of the data subjects over their data or a crucial instrument for the data subjects to exploit the economic value of their data. It may indeed be argued whether this entails that the RtDP is a first step towards the idea of data ownership or property.

This is not the place to open a new discussion on such a well-known and highly debated topic. Serious doubts can be raised, however, about the correctness of such a conclusion at least and especially when dealing with personal data. Personal data, understood, according to the definition in Art. 4 no. 1 GDPR, as any 'information concerning an identified or identifiable person', is, first and foremost and consistently, an attribute that defines personality. Only in some cases can it simultaneously also involve economically relevant profiles, for the data subject himself and herself

---

[27] *Piraino*, Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato, Nuove leggi civili commentate 2017, Vol. 40 Iss. 2, 369 (399), who highlights how the RtDP implies 'the recognition of a typical power of disposition, such as the prerogative to transfer to third parties the right to exploit an entity over which one can exercise a control that prevails over the interest of others in exclusive use'.

[28] *Somaini*, Rivista di diritto dei media 2018, Iss. 3, 164 (174 et seq.).

[29] *Ricci*, in: Finocchiaro, Regolamento, 179 (219).

[30] See *Bravo*, Il 'diritto' a trattare dati personali nello svolgimento dell'attività economica, 2018, 187 et seqq.

and/or others, due to the presence of additional interests. The patrimonial dimension of personal data is, therefore, not a steady feature but only a possible one.[31]

With specific regard to the RtDP, in any case, the prevailing view excludes that the germs of a legal concept of personal data ownership can be seen in such a right.[32] Personal data portability is instead mainly recognised as a user-centred tool, a pillar for the development of personal information management systems (PIMS)[33] or, by another expression, an expression of a human-centred approach to data that contributes concretely to the protection of fundamental rights and interests (health, post-mortem protection of personality, altruistic purposes).[34] In a similar vein is the European Declaration on Digital Rights and Principles for the Digital Decade of 15 December 2022, which defines portability as one of the main pillars on which the EU institutions are committed in the field of protection of digital rights.

These remarks do not eliminate, however, the economic dimension of data portability. Albeit without having a legal declination in terms of ownership, this dimension is clearly present and mainly places the RtDP among the main tools to foster digital data markets. The market protection perspective emerges clearly if one considers the further function of the right to data portability in promoting competition.

In a vision attentive to the needs of the market, the RtDP by enabling the data subjects to reuse their data with other data controllers and removing any constraint, including technical limitations, that binds them to the service offered by their current providers, allows to rebalance the relationship between the data controller and the

---

[31] This patrimonial component is more evident when personal data are in relation to other assets or patrimonial rights, to which they are instrumental, such as interests in an advertising return, the commercialization of an intellectual work or access to banking information. It is far less obvious, however, when, lacking such a correlation, personal data come into consideration only insofar as they represent, if at all, the consideration for the exchange of products and services offered in the online marketplace, representing, for the relevant providers, a source of economic advantage.

[32] The thesis affirming personal data as assets liable to appropriation and, therefore, of property, with the application of the corresponding instruments of protection, is firmly rejected in Italy by a prominent doctrine (*Messinetti*, Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali, Rivista critica di diritto privato 1997, Vol. 15 Iss. 3, 339 (339 et seq.); but see, in a different perspective, *Zeno Zencovich*, Sull'informazione come „bene" (e sul metodo del dibattito giuridico), Rivista critica di diritto privato 1997, Vol. 15 Iss. 3, 485 (485 et seqq.). However, fuelled again precisely by the European Regulation, it finds, especially beyond the Italian borders, a discrete following, even if more often only in the perspective of a possible legislative reform aimed at introducing a property right on data (similar to a new intellectual property right). On the topic see, e. g., *Dorner*, Big Data und „Dateneigentum", Computer und Recht 2014, Vol. 30 Iss. 9, 617; *Kilian*, Property Rights und Datenschutz. Strukturwandel der Privatheit durch elektronische Märkte, in: Festschrift für Christian Kirchner, 2015, 901; *Kerber*, A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis, GRUR Int. 2016, Vol. 65 Iss. 11, 989.

[33] *Copetti Cravo*, How to Make Data Portability Right More Meaningful for Data Subjects? European Data Protection Law Review 2022, Vol. 8 Iss. 1, 52 (53); *Krämer/Senellart/de Streel*, Making data Portability More Effective for The Digital Economy, Centre on Regulation in Europe (Cerre), 2020, 6 (45), available at SSRN: https://ssrn.com/abstract=3866495 (last accessed on: 1 September 2024).

[34] *Copetti Cravo*, European Data Protection Law Review 2022, Vol. 8 Iss. 1, 52 (53).

data subject.[35] It eliminates the advantageous position acquired by the data controller and revitalises the mechanisms of optimal choice on which a fully competitive market is ideally based.

The right to data portability aims, therefore, at minimizing (and, where possible, neutralizing) the potential effects of what, in language borrowed from economics, is known as 'lock-in' effects, i. e., the constraints that bind the consumer to a given company and prevent him or her from turning to other market players to obtain from them better services or services offered on more favourable economic terms. The removal of such constraints has the effect of incentivizing data controllers to compete with each other on quality and price of the services exclusively.[36]

From this point of view, Art. 20 of the GDPR presents, albeit within a complex functionality, a similar rationale to the one inspiring protection of the consumer as the weaker party. The data subject is here seen first and foremost as a consumer or user[37] instead as the holder of a fundamental human right.[38]

This aspect is amply taken into account in the Guidelines of 13 December 2016 on data portability by the *Article 29 Working Party* (WP29), where it is also pointed out that the RtDP represents (among its other purposes) a remedy against a position of weakness or economic dependence of the data subject, consisting in an impossibility, induced also by technical factors, to find an alternative service provider.

What emerges from this is an intrinsic ambiguity of the new instrument of protection. For this reason, some interpreters have expressed perplexity as to the very adequacy of the right to data portability to achieve its multiple purposes, both question-

---

[35] This is emphasised in the Guidelines of the *Article 29 Working Group on Data Protection (WP29)*, Guidelines on the right to data portability, adopted 13 December 2016, vers. amended and adopted 5 April 2017, 16/IT, WP 242 rev.01, 4. Available at https://ec.europa.eu/newsroom/article29/items/611233 (last accessed on: 1 September 2024).

[36] In this, the novelty we are talking about is in close continuity with the already mentioned right to telephone number portability, which allows one to keep one's telephone number when changing operators. As rec. 40 of the directive above 2002/22/EC (the so-called 'universal service directive') states, 'number portability is, in fact, a key element in facilitating consumer choice and effective competition in the competitive telecommunications environment'. See *Graef/Husovec/Purtova*, Data Portability and Data Control: Lessons for an Emerging Concept in EU Law, German Law Journal 2018, Vol. 19 Iss. 6, 1359, and *Ricci*, in: Finocchiaro, Regolamento, 179 (220 et seqq.).

[37] This is also noted by *Ricci*, in: Finocchiaro, Regolamento, 179 (220), for whom portability is indeed 'an instrument for the protection of personal data', but also 'for the free use of a service'.

[38] One may even wonder whether the RtDP should not rather be regulated in the context of consumer law and thus be regulated with the instruments provided for in that context. This was not by chance the choice that was initially made by the French legislator, who, with *Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique* had amended the *Code de la Consommation* (*Loi n° 93-949 du 26 Juillet 1993*) by introducing a general *droit à la portabilité et à la récupération des données* (article L. 224-42-1 et seqq.), which, while providing for an autonomous regulation, nevertheless referred back to the EU Data Protection Regulation as to the modalities of exercising the right. Subsequently, the French legislature, however, retraced its steps by repealing (by *loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles*) the provision introduced in the *Code de la Consommation* in order to avoid possible conflicts between two largely overlapping regulations.

ing its actual potential in terms of protecting the competitive market and highlighting its inconsistency and even harmfulness in terms of protecting the fundamental interests of the individual. Therefore, the first line of criticism aimed to demonstrate how the effectiveness of this instrument to achieve the goal of promoting competition is doubtful, since it is eccentric even with respect to that goal.[39]

The other side of the criticism concerns the compatibility between this instrument and the same fundamental need to protect the personal sphere of the person concerned from external aggression. Indeed, it is emphasised that data portability may hurt the protection of privacy, first of all, because exporting data from one platform to another does not necessarily mean transferring them to a platform that guarantees higher levels of data protection (or at least a level of protection comparable to that of the original platform).[40] Moreover, portability provides an incentive for data controllers to adopt, as far as possible, data processing formats that facilitate the transfer of data and are characterised by interoperability:[41] all phenomena that may make it easier to breach or steal personal data and that multiply the risks of data breaches instead of reducing them.[42] The same can be said from the perspective of the data subjects, since the very existence of the portability tool encourages risky behaviour, for oneself and for one's digital identity, such as the mass transfer of one's data: behaviour that should therefore be limited and not, on the contrary, encouraged. The exercise of the new right, entailing the mobilization of huge masses of data, is therefore capable of undermining the security of personal data by increasing the possibility of a breach and constituting a threat to the privacy of the data subject.

All these criticisms capture the underlying legal problem. The facilitation of the mass transfer of personal data through interoperable formats or formats that, in any case, allow for the easy and rapid reuse of such data is in patent conflict with the principle of data minimisation, which is one of the founding principles of the entire European data protection framework, expressly mentioned, both in recital 156 and, above all, in Art. 5 para. 1 lit. c of the GDPR, which states that data must be 'adequate,

---

[39] See *Weber*, Data portability and big data analytics. New competition policy challenges, Concorrenza e Mercato 2016, 59 (67 et seq.). See also *Krämer/Senellart/de Streel*, Making Data Portability more effective for the Digital Economy, Centre on Regulation in Europe (Cerre), 2020, 55 et seqq., and 272 et seqq., available at https://ssrn.com/abstract=3866495 (last accessed on: 1 September 2024). According to these authors, the RtDP is largely ineffective vis-à-vis to counteract lock-in situations generated by the so-called network effect, arising whenever a consumer's value of a good or service depends on how many other consumers are using the same good or service. The ineffectiveness depends on the fact that the RtDP only targets individual data sets, instead of the whole data subjects' identity profiles, which include their connections with other people. Only if these connections (friends, followers, etc.) were encompassed, would portability reach its goal.

[40] *Weber*, Concorrenza e Mercato 2016, 59 (68).

[41] See rec. 68 of the Regulation: 'data controllers should be encouraged to develop interoperable formats that enable data portability'. However, it must be emphasised that interoperability is not an obligation for data controllers. See also below.

[42] *Polański*, Some thoughts on data portability in the aftermath of the Cambridge Analytica scandal, Journal of European Consumer and Market Law 2018, Vol. 7 Iss. 4, 141 (145 et seq.).

relevant and limited to what is necessary in relation to the purposes for which they are processed („data minimisation")'.

## VII. The Other Side of the Coin: A Largely Ineffective Right Hampered by Numerous Barriers

It is time, however, to turn back to the original reflection, concerning the low uptake to date of the RtDP in practice, in spite of the broad and multifunctional consideration given to it by the GDPR legislature. One must ask, at this point, what the reasons are for this situation, and the answer lies, as partly anticipated at the outset, in the numerous limitations and obstacles that accompany this regulatory instrument making it, at least to date, largely blunt.[43] Three orders of barriers can be identified, which hold back its implementation: legal, cultural and technical barriers.

### *1. Legal Barriers: The Limited Scope of Application*

A first obstacle is represented by the limited scope of application of the RtDP, which derives from the convergence of four limitations: i. the portable Data according to the GDPR are only personal data clearly referable to the person who invokes the right and provided to a controller by the data subject; ii. the legal basis of the processing is restricted to consent or contract; iii. further limitations are due to the protection of other rights;[44] iv. finally, for the data to be ported, the processing must be performed by automated means.

#### *a) A Restricted Set of Portable Data Covered by the RtDP*

To be covered by the right to portability, data shall be personal data *clearly referable* to the person who invokes the right and provided by the *data subject.* Hence the inapplicability of this measure to anonymous or anonymised data, which are not (or are no more) referable to a specific data subject, while its applicability to pseudonymous

---

[43] 'A blunt sword': *Kuebler-Wachendorff et al.*, Informatik Spektrum 2021, Vol. 44, 264 (268 et seq.).

[44] Another limitation to portability is that the right does not exist when the processing is necessary for the performance of a task carried out in the public interest or in connection with the exercise of official authority vested in the data controller. On this point, however, the *Article 29 Working Party* Guidelines have stated that even in these cases, where the public interest prevails, it is nevertheless desirable that good practices be established whereby the data controller puts in place processes that can automatically meet any request for data transfer. Consider, for example, systems that allow the data subject to receive data from the government on the income taxes he or she has paid over the years: *WP29*, Guidelines on the right to data portability, 8. The guidelines thus seem to opt, albeit on the level of optional affirmation of good practices, for the maximum expansion of the scope of the right to portability, with an underlying tendency that seems to unduly favour the circulation of data over the need for privacy protection of the data subject.

data does not seem to be ruled out, since these are data that remain linkable, albeit with certain expedients, to a specific data subject.[45]

More controversial is the requirement regarding the origin of the data from the data subject. The fact that it must be data 'provided by the data subject' inevitably leads to the assumption that the data controller is not obliged to comply with requests for portability with respect to data that the data controller itself has derived independently on the basis of further processing of raw data provided by the data subject[46] (so-called 'inferred' or 'derived' data, i. e., drawn by inference from data processed primarily on provision by the data subject).

It is not clear, however, whether the concept of data provided by the data subject is to be understood in a narrow sense, that is with reference to data that the data subject has knowingly surrendered to the data controller, or in a broad sense, as referring to all data that the data controller obtains including through observation of the activities carried out by the data subject in benefiting from the service. In this regard, the WP29 has favoured the more expansive interpretation,[47] aimed at including 'observed data' within the scope of portability, but the conclusion may raise some doubts, especially considering the greater risks that extending this scope entails for the protection of the data subject's personal data.[48] A reading in accordance with the general principles of the Regulation, and in particular in accordance with the principle of minimization, as well as the careful consideration of a proper balance between protecting the fundamental interest in privacy and protecting economic and market rights, should probably lead to a different conclusion.

*b) A Restricted Legal Basis*

Regarding the legal basis, under Art. 20, the portability rule applies only in cases where the processing is based on the consent of the data subject[49] or is necessary because of the contract (e. g., in the case of a list of songs purchased through an online service).[50] By contrast, other legal bases are not relevant and the data processed in

[45] Pseudonymous data are personal data under the GDPR. They refer to a natural person that can be identified only through additional information that is kept separately. The controller is not obliged to maintain, acquire, or process additional information in order to (re)identify the data subject (Art. 11 para. 1 GDPR).

[46] Think of the heartbeat as examples of raw data, from which, with appropriate algorithmic reprocessing, it is possible to derive information regarding the health status or habits of the data subject. The distinction is also referred to by the *Article 29 Working Party*, which distinguishes precisely between 'observed data' and 'inferential data', only the former included in the scope of the right to portability (but see, on this point, also in the text).

[47] *WP29*, Guidelines on the right to data portability, 9 et seq. The view is shared by *Krämer*, Journal of Competition Law & Technologies 2020, Vol. 17, 290.

[48] Nor should it be overlooked that the distinction between observed personal data and inferential data is, in practice, extremely blurred (see *Pezza*, in: Riccio/Scorza/Belisario, GDPR, 2018, Art. 13 GDPR 204) and thus a harbinger of significant difficulties.

[49] Consent shall be explicit in case of special categories of data (e. g. data concerning health).

[50] Under Art. 20 para. 1 GDPR, the right is recognised only 'where: (a) the processing is based

compliance with them do not fall within the scope of application of the RtDP. Hence, the RtDP does not apply in cases where the processing is based on the legitimate interest of the data controller under Art. 6 para. 1 lit. f GDPR, such as in direct marketing cases.[51] This is presumably an exhaustive enumeration, especially if one values in the interpretation – as we believe is necessary – the hermeneutical criterion aimed at harmonizing the provision with the general principle of data minimization.[52]

*c) Further Limitations Aimed at Protecting Other Rights*

Further limitations are aimed at protecting other rights, both of the data subject and of third parties. As concerns the data subject's rights, according to Art. 20 para. 3 GDPR, the exercise of the right referred to in para. 1 of this Article shall be without prejudice to Art. 17 GDPR, that is to the exercise of the right to erasure. This means that transmission of a set of data does not automatically imply a request for erasure by the transmitting controller.[53] The conclusion is confirmed by recital 68.[54]

Also, the data subject does not lose the right to use the service provided by the transmitting data controller. This means that the exercise of the right does not entail the termination of the contractual relationship between the data subject and the transmitting data controller. It should be noted that portability is not in itself a legal basis justifying processing at the new controller, who must therefore have a new legal basis (as a rule, the consent of the data subject exercising the right).

As to the limitations aimed at protecting rights of others, Art. 20 para. 4 GDPR states that 'The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others'. These may be both data controller's rights or rights of persons different from the data controller. This is undoubtedly the most incisive limitation to RtDP. A further friction profile with respect to the instance of personal pro-

---

on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1)', i. e. when data processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject before entering into a contract.

[51] Art. 20 para. 3 sent. 2 GDPR: 'That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'. And see also rec. 68: 'It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller'.

[52] According to *Bravo*, Il 'diritto', 2018, 216 et seq., the balancing that the Regulation imposes on the interpreter cannot be considered as informed by a principle of abstract prevalence of the interests of the person over those of the market, according to a purely personalistic logic.

[53] However, the obligation may arise from the principle of data minimization pursuant to Art. 5 para. 1 lit. c GDPR.

[54] 'Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract […]'.

tection is grafted in here. In fact, the inherent complexity and relationality of personal data, which in many cases involve multiple data subjects at the same time (think of photos, bank data, online reviews, just to mention a few examples)[55] makes such an assessment extremely delicate and also, in practice, difficult to implement.

According to the WP29, the criterion must be identified in the *personal purpose* of the collection and subsequent processing and the continuing instrumentality of the data in pursuit of that purpose (e. g., the list of contacts in the telephone register).[56] Thus, the transfer of information containing personal data of third parties other than the data subject should be permitted only if the data are processed for personal purposes of the data subject, not if they are used by the new owner to promote its own products or services. In any case, the WP29 has recommended implementing technical tools that allow the data subject to select only the relevant data necessary to meet his or her personal needs to the exclusion of those that may prejudice third parties.

As can be easily guessed, however, the criteria thus developed are marked by an ineradicable rate of vagueness, which makes their application exceedingly uncertain. It is, in fact, inherently arduous to disentangle cases in which there may be prejudice to third parties from those in which such prejudice is *a priori* excluded, as well as to determine whether there is in fact a personal purpose of the person concerned.[57]

The rights of third parties are first and foremost the rights protected by the Regulation itself, i. e., the right to the protection of personal data of third parties with respect to the data subject, considered as a whole and in the individual legal prerogatives in which it is embodied (right to access, right to be forgotten, right to object to processing, etc.).

---

[55] See rec. 68 'Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation'.

[56] *WP29*, Guidelines on the right to data portability, 13: 'In order to avoid adversely affecting the rights and freedoms of the third parties concerned, the processing of the personal data in question by a different data controller is permissible only to the extent that the data remain in the exclusive possession of the user who had requested their portability and are used exclusively for personal or domestic purposes. The „new" owner who has received such data (even directly, if the user so requests) may not use the data referring to third parties for its own purposes-for example, to propose *marketing* offers and services to said third parties, or to enrich the profile of the third parties concerned and reconstruct their social context without their knowledge and consent. Nor can it use them to derive information about the third parties in question and create specific profiles, even if it already holds their personal data. Otherwise, the processing is likely to be unlawful and in violation of the principle of fairness, especially if the third parties in question do not receive information and are unable to exercise the rights granted to them as those affected by the processing.'

[57] See *Somaini*, Rivista di diritto dei media 2018, Iss. 3, 164 (184): 'In practice, it will be for the courts to establish on a case-by-case basis whether the exercise of data portability adversely impacts third-party rights in each specific circumstance. In sum, it appears that the GDPR may have underestimated the number of conflicts involving third-party rights and this provision, contingent upon the interpretation that will be adopted by the European Data Protection Board and settled by the courts, may significantly impair the reach of the right.'

When portability implies transmission of personal data belonging to third parties, this processing must be subject to the same legitimacy prerequisites as under the Regulation in general, i. e., it will have to find a specific and distinct legal basis (e. g., consent).[58] According to the WP29, it is up to the data controller to assess on a case-by-case basis the relevance and non-excessive nature of the data being transferred.

Different conclusions should be reached, however, if the exercise of the right to portability might affect others' intellectual property rights or trade secrets. In this case, again according to the WP29 Guidelines, the balance should not necessarily be unfavourable to the right to data portability, i. e., lead to its exercise being denied.[59] It is believed, however, that others' intellectual property rights might require that the concrete ways of exercising the right be adjusted to respect the rights of others,[60] again with an assessment *in concreto* that cannot be predicted in its outcomes.

### *2. Cultural Barriers*

From a cultural point of view, it is sufficient to recall what has already been highlighted above, namely, the lack of awareness of the instrument on the part of the data subjects and the limited understanding of how it actually works, also because of the limited user-friendly nature of the existing portability tools.[61] Even from the business perspective, however, there is still little awareness of the existence of the right to portability and of the technical tools that need to be adopted in order to be ready to respond to portability requests. Costs are a further constraint in this direction.

### *3. Technical Barriers*

The last barrier to the correct and effective application of data portability lies in the restrictive and uncertain regulation of its technical requirements. As a first limita-

---

[58] See, on this point, *WP29*, Guidelines on the right to data portability, 12: 'If the portable data contain personal information referring to third parties, a different basis of lawfulness must be identified for their processing: for example, the controller to whom the data are transferred may be pursuing a legitimate interest (within the meaning of Article 6(1)(f)), in particular if the processing carried out by the new controller aims at providing a service to the data subject to enable him or her to process personal data in the context of exclusively personal or family activities.' On this point see also *Somaini*, Rivista di diritto dei media 2018, Iss. 3, 164 (182).

[59] See, on this point, *WP29*, Guidelines on the right to data portability, 14: 'although it is appropriate to take the rights in question into account before responding to a request for portability, such considerations should not lead to a denial to provide the data subject with all the information. In addition, the data controller should not reject a portability request on the grounds of the violation of another contractual right-for example, because of the existence of arrears or a commercial dispute with the data subject […]. However, the existence of a potential risk to business activity cannot, in isolation and as such, be a basis for denying a portability request: data controllers may transmit personal data provided by data subjects in a format that does not reveal confidential business information or information subject to intellectual property rights.'

[60] *Pezza*, in: Riccio/Scorza/Belisario, GDPR, 2018, Art. 13 GDPR 207.

[61] *Kuebler-Wachendorff et al.*, Informatik Spektrum 2021, Vol. 44, 264 (266 et seqq.).

tion, portability is only restricted to data processed with automated means. Hence, as the WP29 notes,[62] it does not apply to most paper archives or records.

Furthermore, according to Art. 20 para. 1 and 2 GDPR, data should be transmitted 'in a structured, commonly used and machine-readable format […] without hindrance'. In the case of direct transmission from one controller to another (Art. 20 para. 2 GDPR), 'the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible'.

However, there are no mandated technical indications. This lack, albeit consistent with the principle of technological neutrality with regard to the means of transmission, undoubtedly leads to uncertainties.

According to recital 68 'Data controllers should be encouraged to develop interoperable formats that enable data portability'. Interoperability, in this context meaning, according to WP29 (that refers to ISO/IEC 2382-01), 'the capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units'[63] is, therefore, a 'desired outcome' of the minimal requirements (interoperable formats) outlined in Art. 20 GDPR, not a necessary result.[64]

Interoperability, anyway, even if it were achieved, would not mean (full) compatibility. Interoperable systems are able to receive data and process them further to make them compatible with their purposes. Compatible systems, instead, send and receive data that are ready to use for both the original controller and the new one. According to recital 68, 'The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible'. As the WP29 puts it, 'Portability aims to produce interoperable systems, not compatible systems'.

Furthermore, in the case of direct transmission of data from one controller to another (Art. 20 para. 2 GDPR), portability is possible only when the receiving controller supports the data format, but there is no obligation for the latter to support it. The concept is, therefore, that of 'technical feasibility', based on a mere possibility and undoubtedly vague and uncertain.

Finally, data shall be transmitted 'without hindrance'. This concept is a bit less vague and should include both legal hindrance, like contractual clauses that restrict the data subject's right or make it conditional on certain events, financial hindrance, like fees, technical hindrance, like lack of interoperability, deliberate obfuscation etc.

---

62 *WP29*, Guidelines on the right to data portability, 10.

63 Interoperability is also a key concept in the DMA (Regulation 2022/1925, Digital Markets Act), where it is defined (Art. 2 para. 29 DMA) as 'The ability to exchange information and mutually use the information which has been exchanged through interfaces or other solutions, so that all elements of hardware or software work with other hardware and software and with users in all the ways in which they are intended to function'. Under the DMA (Art. 6 para. 7), interoperability constitutes a general obligation for gatekeepers. On this subject see below *Gatti*, in this volume.

64 On the different forms of interoperability form the technical point of view see *Kranz et al.*, Data Portability, Business & Information Systems Engineering 2023, Vol. 65 Iss. 5, 597 (601 et seqq.).

## VIII. The Weople Case (Before the Italian Competition Authority, AGCM)

The lack of interoperability came to the attention as a possible consequence of an abuse of a dominant position in a case that went before the Italian competition authority (*Autorità garante della Concorrenza e del Mercato*, AGCM). The case concerned the app 'Weople', launched in 2018 by an Italian company named Hoda. Weople presents itself as a data broker, that is as an intermediary between data subjects/data owners and data users, acting (at least nominally) in favour and on behalf of the first ones to obtain a profit and transfer it to them after deducting a commission. As one can read from the company's webpage, Weople offers its customers to open a personal bank vault, that is 'a secure, protected space where [they] can deposit [their] digital data and have control over it at all times.' The company also commits itself to activate the customer's rights on their data, among them also the right to data portability, and give them back possession of their data and invest them.[65]

In 2019, Hoda turned to the Italian Privacy Supervisor, complaining for the refusal by many companies to let Weople exercise its users' rights to portability. Without responding to Hoda, the Italian Supervisor asked the European Data Protection Board (EDPB) for an opinion, which, however, was never rendered.

In the meanwhile, Weople filed a complaint against Google-Alphabet because Google was making it excessively difficult for its users to exercise their right to portability to transfer their data to Weople. In fact, the procedure put in place by Google to respond to portability requests (based on the tool *Google Takeout*) appeared to be too slow and complex, thus discouraging users from taking the initiative.

Therefore, the Italian AGCM opened a procedure against Google, and finally, in 2023, Google made several commitments to comply with the Authority's guidance. Google's commitments were then accepted by the AGCM in July 2023. These commitments include: making available a link to be embedded in third-party applications to allow data subjects to download and share personal data with them (one-time or periodically); creating a sandbox to test a direct portability service through an API (Application Programming Interface) mechanism (Art. 20 para. 2 GDPR).

The Weople case has raised some new issues that need to be addressed, concerning the possible exercise of data portability by data intermediaries (so-called 'infomediaries'): There is, above all, a risk of over-concentration of personal data in the same entity. Permitting intermediaries to activate the rights of a high number of different data subjects places them in the position of gathering personal data and, potentially, harvesting them. This is more than true if one considers that the data involved are not only data processed by online service providers but also, potentially, economic and

[65] 'With Weople, you can take back possession of all your data, deposit and invest it in your personal bank vault and access it whenever you want' (Weople's website). In essence, Weople asks its users for a mandate to claim data that other companies have collected about them, and then store it in a digital wallet. The users can thus monetise the data deposited in Weople's accounts.

financial data, health data, sensible data, etc. Given the width and generality of the data involved, this may raise concern also about the validity of the consent provided to the intermediary by the data subject. Moreover, a risk of conflicts of interest arises, especially between economic interests, on one side, and the protection of data subjects' rights and freedoms, on the other side.

The Data Governance Act (DGA)[66] takes these risks into account and attempts to limit them, in particular by adopting the principle of intermediary neutrality (see recital 33: 'It is therefore necessary that data intermediation services providers act only as intermediaries in the transactions, and do not use the data exchanged for any other purpose';[67] and Art. 12 lit. a DGA[68]). The role of intermediaries in the relationship between controllers and data subjects is finally also recognised by the EDPB Guidelines 01/2022 on data subject rights – Right of access.[69]

In theory, many of the concerns have therefore been overcome. In practice, however, given the difficulty to transform the principle of neutrality in practice, the exercise of the RtDP by intermediaries still remains a critical issue.

## IX. An Interlocutory Conclusion

The evolution of the right to data portability subsequent to the GDPR goes in the direction of overcoming the limitations and certain contradictions that characterise the original version of Art. 20 GDPR. However, an in-depth analysis of this evolution, for which we refer to in a separate contribution,[70] will show that in no case has the will

---

[66] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJEU L 152/1, 3.6.2022.

[67] See also rec. 30: 'A specific category of data intermediation services includes providers of services that offer their services to data subjects. Such data intermediation services providers seek to enhance the agency of data subjects, and in particular individuals' control over data relating to them. Such providers would assist individuals in exercising their rights under Regulation (EU) 2016/679, in particular giving and withdrawing their consent to data processing, the right of access to their own data, the right to the rectification of inaccurate personal data, the right of erasure or right „to be forgotten", the right to restrict processing and the right to data portability, which allows data subjects to move their personal data from one data controller to the other. In that context, it is important that the business model of such providers ensures that there are no misaligned incentives that encourage individuals to use such services to make more data relating to them available for processing than would be in their interest'.

[68] Art. 12 DGA: '(a) the data intermediation services provider shall not use the data for which it provides data intermediation services for purposes other than to put them at the disposal of data users and shall provide data intermediation services through a separate legal person; […] (m) the data intermediation services provider offering services to data subjects shall act in the data subjects' best interest where it facilitates the exercise of their rights […]'.

[69] See 3.4 'Requests made via third parties/proxies' 3.4.2, 'Exercising the right of access through portals/channels provided by a third party', particularly 'companies that provide services which enable data subjects to make access requests through a portal'.

[70] See below *Gatti*, in this volume.

of the European legislator been directed toward the elaboration of a draft reform of Art. 20 GDPR. In fact, the steps taken so far or being planned all go in the direction of flanking the instrument envisaged in the GDPR with other similar instruments, mostly of a sectoral nature or having partially different objective (i. e., portable data) and subjective (i. e., right holders) prerequisites.

This asystematic and fragmentary development, precisely because of these characteristics, raises certain perplexities, in that it risks creating overlaps or conflicts of application between largely related instruments. Moreover, it does not remove the structural limitations of the RtDP in its original version in the GDPR, which thus retains all its flaws. Instead, portability would need an organic intervention, aimed at rationalizing and simplifying the existing instruments, possibly bringing them back to unity. Such an intervention, in any case, if it is ever made, cannot disregard the revision of Art. 20 of the GDPR, which must necessarily be the starting point of any reform.

# The Evolution of Data Portability Right(s) after the GDPR

*Stefano Gatti*



## I. Introduction. The Evolution of Data Portability

Since its first appearance in Art. 20 GDPR, the right to data portability is evolving rapidly in European legislation. On the one hand, this evolution involves the data subject's right to access, retrieve, and move data. Data access and portability rights are multiplying, revealing their multifaceted goals[1] in the different frameworks drawn by the legal instruments adopted by the European Union institutions. As a result, the relationship between these new rights and the right to data portability under Art. 20 GDPR could appear to be difficult. In general, the new portability rights *complement* or *strengthen* the basic GDPR right, but they have a narrower scope of application. On the other hand, the establishment of a European single data market took its first steps by assuming the free movement of data (data sharing and data reuse) as a fundamental pillar.

Approaching data as intangible assets that can also be exploited for commercial purposes shifts the focus of portability from strengthening the data subject's control over the information about him or her to increasing the possibilities for data movement in the market. For this reason, it is unsurprising that natural and legal persons other than the data subject can sometimes exercise these new rights.[2] The shareability and 'portability' of data (in a broader sense than the one which the right in Art. 20

[1] Empowering consumers is at the heart of the right to data portability in some of the EU directives protecting them. That is one of the main objectives of data portability, which has been already highlighted in the context of Art. 20 GDPR: See para. 2.

[2] See para. 3 and 4.

GDPR relates to) tends to become the general rule, encompassing both personal and non-personal data. When the data to be ported are personal, the prevalence of the rules protecting them only adds a (complicated) coordination issue. Still, it does not result in an obstacle to data access and porting.

Strengthening the right to data portability enables greater exploitation of the potential of data that benefits not only the market but also personality rights.[3] An example is given by the forth-coming European Health Data Space, where the more far-reaching rights to access and portability are complemented by rules designed to ensure a high level of accessibility and usability of health data.[4]

## II. Consumer Law: Data Portability as a Tool to Empower Consumers

In European consumer law, the right to data portability has recently appeared in the Directives that have modernised consumer protection to keep pace with the digital nature of goods and services offered to consumers.

According to Directive 770/2019/EU, on lack of conformity of digital content and services supplied to consumers, the trader must comply with the obligations under the GDPR when the consumer exercises the remedy to terminate the contract (Art. 16 para. 2 concerning the trader's obligations in the event of termination). This provision embodies a (general and) superfluous rule since there is no doubt that the GDPR[5] applies to these cases and prevails, as expressly stated in Art. 3 para. 8 Directive 770/2019/EU.[6]

However, this provision aims to emphasise that the trader (who is a data controller in the sense of Art. 4 no. 7 GDPR) must process the consumer's personal data after the termination of the contract, according to the legal bases outlined in the GDPR (Art. 6 and 9) and in compliance with the principles enshrined in this Regulation (Art. 5). Furthermore, the trader must respect consumers' rights (as data subjects)[7] over their data. As a result, the consumer can invoke the right to data portability, which means the possibility for him or her to retrieve and reuse the personal data that he or she has provided to the trader (for example, photographs stored in a cloud). The

---

[3] Cf. *A. Laje*, El derecho a la portabilidad de datos como derecho personalísimo, in: Troiano (ed.), Diritto privato e nuove tecnologie. Riflessioni incrociate tra esperienze giuridiche a confronto, 2022, 9 (9 et seqq.).

[4] See para. 5 and 6.

[5] Regulation (EU) 2016/679, General Data Protection Regulation.

[6] 'Union law on the protection of personal data shall apply to any personal data processed in connection with contracts referred to in paragraph 1. In particular, this Directive shall be without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC. In the event of conflict between the provisions of this Directive and Union law on the protection of personal data, the latter prevails.'

[7] Both consumers and data subjects are natural persons by definition: Compare Art. 2 no. 6 Directive (EU) 2019/770 and Art. 4 no. 1 GDPR.

consumer can, therefore, transmit those data to a new trader, that is, to a new data controller.[8]

In this context (i. e. in the context of termination of a consumer's contract), data portability reveals its multiple purposes[9] by strengthening the data subject's control over his or her own data.[10] The main goal is to empower the consumer,[11] who must not be burdened by technical barriers in switching from one supplier to another.[12] As a result, in addition to fostering competition among businesses,[13] the effectiveness of European consumer protection law remedies increases.

Art. 16 para. 4 Directive 770/2019/EU also provides for a consumer right to the portability[14] of any content provided or created by him or her when using the digital content or service purchased ('right of retrieval'[15]). Since digital content that comes to the fore consists of non-personal data[16] this provision is intended to lay down

---

[8] Art. 20 para. 1 GDPR. Where it is 'technical feasible', the consumer can ask the trader directly to transmit his or her data to the new trader (direct portability): Art. 20 para. 2 GDPR. See *Troiano*, Il diritto alla portabilità dei dati, in: Zorzi Galgano (ed.), Persona e mercato dei dati. Riflessioni sul GDPR, 2019, 195 (195 et seqq.).

[9] See *Troiano*, in: Zorzi Galgano, Persona, 195 (199 et seqq.); *Catalano*, Il diritto alla portabilità dei dati tra interessi individuali e prospettiva concorrenziale, Europa e diritto privato 2019, Iss. 3, 833 (837 et seqq.).

[10] See recital 68 GDPR. According to the *European Data Protection Supervisor* (EDPS), Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability, Opinion 7/2015, available at https://www.edps.europa.eu/sites/default/files/publication/15-11-19_big_data_en.pdf (last accessed on: 17 July 2024), allowing data portability 'could […] let individuals benefit from the value created by the use of their personal data'.

[11] *Colangelo/Maggiolino*, From fragile to smart consumers: Shifting paradigm for the digital era, Computer Law & Security Review 2019, Vol. 35 Iss. 2, 173.

[12] Data portability tackles the so-called (data-induced) 'lock-in effect': *Krämer*/*Senellart*/*De Streel*, Making Data Portability more effective for the Digital Economy. Economic Implications and regulatory Challenges, Report, Centre on Regulation in Europe, 2020, 1 (55 et seqq.), available at https://cerre.eu/publications/report-making-data-portability-more-effective-digital-economy/ (last accessed on: 17 July 2024).

[13] Cf. *Battelli*/*D'Ippolito*, Il diritto alla portabilità dei dati personali, in: Tosi (ed.), Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy, 2019, 185 (187 et seqq.).

[14] *Dix*, in: Döhmann/Papakonstantinou/Hornung/De Hert (eds.), General Data Protection Regulation. Article-by-Article Commentary, 2023, Art. 20 GDPR 510. The close relationship between the right to data portability and the right to portability of a different digital content is made clear by the transmission quality standard imposed on the trader according to Art. 16 para. 4: 'The consumer shall be entitled to retrieve that digital content other than personal data free of charge, without hindrance from the trader, within a reasonable time and in a commonly used and machine-readable format'.

[15] *Cámara Lapuente*, Termination of the Contract for the Supply of Digital Content and Services, and Availability of Data: Rights of Retrieval, Portability and Erasure in EU Law and Practice, in: Lohsse/Schluze/Staudenmayer (eds.), Data as Counter-Performance – Contract Law 2.0? 2020, 163 (180 et seqq.).

[16] Digital content other than personal data could be, for example, digital images, video and audio files, the listening history of a music streaming service: recital 69 Directive 2019/770/EU. As long as these data are still referable to the consumer (natural person), they must be considered

backup rules for cases in which the GDPR cannot apply.[17] However, these rules, for reasons that are not entirely clear, limit, in favor of the trader, the scope of this new right in respect to data that can be 'ported' or 'retrieved.'[18] The reference to data 'generated' by users, though, makes it clear that observed data (which falls within the scope of application of data portability under Art. 20 GDPR only if the expression 'provided data' is interpreted in a broad sense)[19] are included.

The same provisions were later taken up by Art. 13 para. 4, 6, and 7 Directive 2011/83/EU as amended by Directive 2019/2161/EU,[20] concerning the regulation of distance and off-premises contracts, for the case in which the contract concerns digital content or services and the consumer exercises his or her right of withdrawal (*ius poenitendi*). In these cases, which also involve the termination of the contract, the same purposes mentioned above (to prevent the lock-in effect of the consumer and to ensure the effectiveness of remedies) are reiterated.

## III. The Right to Data Portability in the Logic of the Market. The Digital Markets Act

Limitations that constrain data portability under Art. 20 GDPR can hinder free competition among businesses. Furthermore, the consumer's lock-in effect is not prevented if the possibility for the receiving controller to reuse the data is not guaranteed (lack of interoperability). Indeed, personal and non-personal data availability is an essential precondition for businesses to strengthen their position in the digital market.[21] This explains why, conversely, the monopoly on data by large firms offering

personal data, with the result that the consumer, as a data subject, can exercise the right to data portability, pursuant to Art. 20 GDPR.

[17] *Sein/Spindler*, The new Directive on Contracts for Supply of Digital Content and Digital Services – Conformity Criteria, Remedies and Modifications – Part 2, European Review of Contract Law 2019, Vol. 15 Iss. 4, 365 (382).

[18] The right to retrieve digital content other than personal data cannot be exercised where such content: '(a) has no utility outside the context of the digital content or digital service supplied by the trader; (b) only relates to the consumer's activity when using the digital content or digital service supplied by the trader; (c) has been aggregated with other data by the trader and cannot be disaggregated or only with disproportionate efforts'. These limitations have been criticised by some Scholars: See *A. Metzger/Efroni/Mischau/J. Metzger*, Data-Related Aspects of the Digital Content Directive, Journal of Intellectual Property, Information Technology and Electronic Commerce Law 2018, Vol. 9 Iss. 1, 90 (104 et seq.).

[19] See *Troiano*, in: Zorzi Galgano, Persona, 195 (212); *Working Party Article 29*, Guidelines on the right to data portability, 9 et seq., available at https://ec.europa.eu/newsroom/article29/items/611233 (last accessed on: 17 July 2024), has come to the conclusion mentioned in the text.

[20] Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules, OJEU L 328/7, 18.12.2019 (so-called *Omnibus* Directive).

[21] 'Data is the lifeblood of economic development': Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Commit-

core platform services[22] is a significant cause of their enormous power in the digital market, which hinders the entry of new competitors.[23]

The European legislator adopted the *Digital Markets Act*[24] to counter this phenomenon. In this piece of legislation, among several measures taken to curb the power of large digital platforms, a significant role is played by the right of the user[25] of such platform services to data portability.[26] Compared to Art. 20 GDPR, this right has been extended and strengthened[27] when exercised against a 'gatekeeper'.[28]

Art. 6 para. 9 DMA requires the gatekeeper to ensure effective data portability to end users. In practice, end users must be provided with full accessibility and usability of the data for which they request access or transmission.[29]

Compared to Art. 20 GDPR, the limitations of data portability on the legal basis of their processing vanish. Data covered by the right are no longer exclusively those 'provided' by the requesting end user but also include those 'generated through the activity of the end user in the context of the use of the relevant core platform service.'

---

tee of the Regions 'A European strategy for data', Brussels, 19.2.2020, COM(2020) 66 final, 3, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066 (last accessed on: 17 July 2024). Cf. also *Resta*, Pubblico, privato, collettivo nel sistema europeo di governo dei dati, Rivista trimestrale di diritto pubblico 2022, Iss. 4, 971 (973 et seqq.).

[22] Core platform services are defined by Art. 2 para. 2 DMA (fn. 24). This notion includes: (a) online intermediation services; (b) online search engines; (c) online social networking services; (d) video-sharing platform services; (e) number-independent interpersonal communications services; (f) operating systems; (g) web browsers; (h) virtual assistants; (i) cloud computing services; (j) online advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by an undertaking that provides any of the core platform services listed in lit. a to i.

[23] *Kuebler-Wachendorff et al.*, The Right to Data Portability: conception, status quo, and future directions, Informatik Spektrum 2021, Vol. 44, 264 (265).

[24] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJEU L 265/1, 12.10.2022. It entered to force on 1 November 2022 and applies from 2 May 2023.

[25] Users can be divided into 'business users' and 'end users'. 'Business users' are enterprises that use platform services to reach their customers (Art. 2 no. 21 DMA: 'natural or legal person acting in a commercial or professional capacity using core platform services for the purpose of or in the course of providing goods or services to end users'). 'End users' are everyone else, including business users' customers (Art. 2 no. 20 DMA).

[26] 'For the avoidance of doubt, the obligation on the gatekeeper to ensure effective portability of data under this Regulation complements the right to data portability under the Regulation (EU) 2016/679.' (recital 59 DMA).

[27] See *Da Rosa Lazarotto*, The right to data portability: A holistic analysis of GDPR, DMA and the Data Act, European Journal of Law and Technology 2024, Vol. 15 Iss. 1, 1 (8 et seq.), available at https://ejlt.org/index.php/ejlt/article/view/988 (last accessed on: 17 July 2024).

[28] 'Gatekeeper' is a label that, based on certain indicators, is assigned by the EU Commission to the largest digital market players (Art. 3 DMA). From this qualification derive specific additional obligations (Art. 5–7 DMA) that these undertakings must meet in carrying out their business activities.

[29] Recital 59 DMA: 'The data should be received in a format that can be immediately and effectively accessed and used by the end user or the relevant third party authorised by the end user to which the data is ported.'

In light of this definition, portable data also include non-personal data, as long as they are related to the use of the platform service.

The technical quality of data portability is set at a significantly higher level than the basic version of Art. 20 GDPR: it is necessary to ensure the promptness of transmission from the request (*real-time* portability) and the continuity of data flow from the platform to the end user or authorised third party (*continuous* portability[30]).[31]

Such an evolution of the right to data portability has also been advocated by some scholars in the general context of personal data protection.[32] However, the European choice to burden only large undertakings with these technical standards can be welcomed, since costs related to such standards could have damaged the smallest competitors in the market.[33] The same portability right has been recognised to third parties appointed by the data subject, according to the idea that data subjects' rights can also be exercised by persons appointed by them.[34]

Art. 6 para. 10 DMA goes further, stating that accessibility and usability of data must also be granted to business users concerning their customers' data.[35] In this case, data portability can refer even to the personal data of end users who have used

[30] *Continuous* portability means that a repeated request for data is not necessary from the data subject: this way of exercising the right to data portability makes multihoming possible, which entails the possibility for consumers of benefiting from several platform services at the same time, rather than migrating from one to another. According to recital 69, 'facilitating switching or multi-homing should lead, in turn, to an increased choice for end users and acts as an incentive for gatekeepers and business users to innovate.'

[31] Pursuant to Art. 6 para. 9 DMA, the gatekeeper should provide, 'free of charge, tools to facilitate the effective exercise of such data portability'. This part of the provision is explained by recital 59 DMA: 'Gatekeepers should also ensure, by means of appropriate and high-quality technical measures, such as application programming interfaces, that end users or third parties authorised by end users can freely port the data continuously and in real time'. Application Programming Interfaces (APIs, 'interfaces of applications or web services made available by data controllers so that other systems or applications can link and work with their systems') have also been encouraged by WP29 Guidelines, 15. In short, the purpose is to make data portability a 'plug-and-play right': *Da Rosa Lazarotto*, European Journal of Law and Technology 2024, Vol. 15 Iss. 1, 1 (8 et seq.).

[32] *Krämer*, Personal Data Portability In The Platform Economy: Economic Implications And Policy Recommendations, Journal of Competition Law & Technologies 2020, Vol. 17 Iss. 2, 263 (296).

[33] The danger of incentivizing data migration practices, including through economic incentives, to less secure digital environments (*Krämer*, Journal of Competition Law & Economics 2020, Vol. 17 Iss. 2, 263 [297]; *Troiano*, in: Zorzi Galgano, Persona, 195 [210]) still remains.

[34] The question of whether GDPR rights can be exercised by third parties authorized by data subjects seems to have found a positive solution in the drafting history of the Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJEU L 152/1, 3.6.2022. See *Bravo*, Le cooperative di dati, Contratto e impresa 2023, Vol. 39 Iss. 3, 757 (791 et seqq.). However, lack of clarity on this point has been criticised by *Resta*, Rivista trimestrale di diritto pubblico 2022, Iss. 4, 971 (991 et seqq.).

[35] A further sharing obligation relates to certain data generated by end users on the gatekeeper's online search engines ('ranking, query, click and view data'): the gatekeeper must grant search engine service providers who request it, access 'on fair, reasonable and non-discriminatory terms' to such data: Art. 6 para. 11 DMA.

the product or service offered by the requesting business user through the platform service operated by the gatekeeper. The data involved, therefore, can be personal data of third parties, and this version of data portability can be seen as a prerogative of a party that qualifies as a data controller in the framework of the GDPR.[36]

## IV. The Data Act

The latest evolution of data portability, which can be summarised in the fact that parties other than the data subject can take the initiative for data access and sharing, moves this right away from its original setting in Art. 20 GDPR. In these cases, the purpose of data portability is not just to strengthen the control of an individual over their own data but to foster data movement and sharing in the market's interest.

This idea aligns with the core of the European Data Strategy,[37] which is to create a Single Data Market.[38] The main pillars of this Strategy are two EU Regulations that have recently entered into force: the Data Governance Act (DGA)[39] and the Data Act (DA).[40] These legal acts move in synergy with the Digital Markets Act, the Digital Services Act (DSA),[41] and the Artificial Intelligence Act (AI Act),[42] drawing the

---

[36] For this reason, Art. 6 para. 10 DMA specifies that 'With regard to personal data, the gatekeeper shall provide for such access to, and use of, personal data only where the data are directly connected with the use effectuated by the end users in respect of the products or services offered by the relevant business user through the relevant core platform service, and when the end users opt in to such sharing by giving their consent.'

[37] EU Commission Communication 'A European strategy for data' (fn. 21).

[38] EU Commission Communication 'A European strategy for data' (fn. 21), 6: 'The aim is to create a single European data space – a genuine single market for data, open to data from across the world – where personal as well as non-personal data, including sensitive business data, are secure and businesses also have easy access to an almost infinite amount of high-quality industrial data, boosting growth and creating value, while minimising the human carbon and environmental footprint'.

[39] Regulation (EU) 2022/868 on European data governance and amending Regulation (EU) 2018/1724. This Regulation is applicable from 24 September 2023. See *von Ditfurth/Lienemann*, The Data Governance Act: – Promoting or Restricting Data Intermediaries? Journal of Competition and Regulation in Network Industries 2022, Vol. 23 Iss. 4, 270; *Owusu*, Data sharing in the personal data economy. Does sharing mean caring? European Journal of Privacy Law and Technologies 2023, Iss. 2, 217 (217 et seqq.).

[40] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJEU L 71/1, 22.12.2023. The Regulation will be applicable from 12 September 2025.

[41] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJEU L 277/1, 27.10.2022. This Regulation applies from 17 February 2024.

[42] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJEU L 144/1, 12.7.2024.

framework within which the European economy based on data flow, sharing, and reuse is rapidly developing.[43]

Although the Data Governance Act is dedicated to shaping a legal framework for data intermediation services, it does not create new rights to share data.[44] By contrast, new data access and sharing rights represent the main novelty of the Data Act. This Regulation aims to facilitate the free movement of data generated by connected products and related services, in a word, by the *IoT (Internet of Things)*.[45] By shaping new rights, the specific aims of the Data Act are promoting aftermarket innovations, preventing lock-in effects of users[46] and developing new services based on data.[47]

The critical role is played by the user of such a product or service, who has the right to access and share a wide range of data, including observed data and metadata, that must be made available by the data holder. The 'user' is anyone who owns the connected product or has a temporary right on it.[48] The 'data holder' is the entity (natural or legal person) to whom data collected and generated by smart products and related services are, *de facto*, available.[49]

Both personal and non-personal data can be requested to be shared. Data are generally conceived as 'digitisation of users' actions or events' in connection with IoT.[50] This definition, even if very broad, limits the scope of these new rights.[51] According

---

[43] *Resta*, Rivista trimestrale di diritto pubblico 2022, Iss. 4, 971 (971 et seqq.); *Marino*, Accesso, portabilità e condivisione nella disciplina europea del mercato dei dati, in: Guzzardi (ed.), Persona e mercato nella società digitale, 2024, 19 (53 et seqq.).

[44] *Wolters*, The Influence of the Data Act on the Shifting Balance between Data Protection and the Free Movement of Data, European Journal of Law and Technology 2024, Vol. 15 Iss. 1, 1 (9 et seq.), available at https://ejlt.org/index.php/ejlt/article/view/991 (last accessed on: 17 July 2024).

[45] Cf. *Chiarella/Borgese*, Data Act: New Rules about Fair Access to and use of Data, Athens Journal of Law 2024, Vol. 10 Iss. 1, 47 (52 et seqq.); *Poletti*, Il controllo dell'interessato e la strategia europea sui dati, Osservatorio delle fonti 2023, Iss. 2, 367 (373 et seqq.).

[46] *Metzger*/*Schweitzer*, Shaping Markets: A Critical Evaluation of the Draft Data Act, ZEuP 2023, Iss. 1, 42 (47). According to these Authors, the Data Act's main novelty is the introduction of a 'horizontal' data access right.

[47] Recital 32 DA. See also *Wolters*, European Journal of Law and Technology 2024, Vol. 15 Iss. 1, 1 (18): 'these rights are designed to foster the emergence of liquid, fair and efficient markets for data.'

[48] Art. 2 no. 12 DA. The user can be an individual or a legal entity. It could be a consumer, a business or a public sector body. More persons (such as the owner and the renter) can be qualified ad 'users' at the same time (recital 18 DA).

[49] See *Metzger*/*Schweitzer*, ZEuP 2023, Iss. 1, 42 (54). According to Art. 2 no. 13 DA, 'data holder' is anyone 'that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service'. This definition does not overlap with the GDPR notion of 'data controller'. Involved data are personal data, the data holder may simultaneously qualify as data controller, provided that he or she 'determines the purposes and means of the processing of personal data' (Art. 2 no. 7 GDPR). In any case, Data Act 'should not be interpreted as recognising or conferring any new right on data holders to use data generated by the use of a connected product or related service' (recital 5 DA).

[50] Recital 15 DA.

[51] *Wolters*, European Journal of Law and Technology 2024, Vol. 15 Iss. 1, 1 (14 et seq.).

to Art. 5 DA, 'upon request of the user, or by a party acting on behalf of a user', the data holder must transmit those data to a third party (a 'data recipient'[52]), who is often the person concretely interested in the data movement.[53] This provision entails a new version of the right to data portability[54] and paves the way for shaping third-party 'derived rights' to data access.[55]

The new right to 'share' data, similar to Art. 20 GDPR, does not cover inferred data, that is, data derived from data actively or passively provided by the data subject. However, pre-processed data, that is, raw data perceived by the connected product or the related services that have been processed to make them understandable and usable, are included. Symmetrically to the right to access (Art. 4 DA), this right refers to 'readily available data' and to 'the relevant metadata necessary to interpret those data'.[56] Quality standards for sharing data with third parties are considerably high to ensure effectiveness and interoperability.[57]

Since the Data Act access rights are conceived in favor of a market logic, their subjective scope of application is accordingly limited. On the one hand, data access cannot be given to gatekeepers;[58] on the other hand, the related obligations do not burden micro and small enterprises (within the meaning of Art. 3 of the Annex to Recommendation 2003/361/EC).[59]

---

[52] Art. 2 no. 14 DA: 'a natural or legal person, acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a connected product or related service, to whom the data holder makes data available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation adopted in accordance with Union law.'

[53] E.g. a business who is interested in the data generated by IoT in order to develop and provide aftermarket services. See *Metzger*/*Schweitzer*, ZEuP 2023, Iss. 1, 42 (58).

[54] Art. 5 DA does not use the terms 'data portability', but it refers to the idea of 'data sharing'. Recital 35 DA clarifies that the right laid down in this Regulation 'complements accordingly the right, provided for in Art. 20 of Regulation (EU) 2016/679', to data portability.

[55] *Metzger*/*Schweitzer*, ZEuP 2023, Iss. 1, 42 (45). In contrast to general portability (*Marino*, in: Guzzardi, Persona, 2024, 19 [47]), Art. 6 DA provides for obligations on third parties who get access to IoT data, that can be exploited 'only for the purposes and under the conditions agreed with the user'. In B2B relationships between data holder and data recipient, the latter may be asked to pay a 'reasonable compensation' to the data holder for making data available (Art. 9 DA, which provides for asymmetric rules protecting SME). According to recital 46 DA, 'such compensation should not be understood to constitute payment for the data itself. The Commission should adopt guidelines on the calculation of reasonable compensation in the data economy.'

[56] 'Readily available data' means 'product data and related service data that a data holder lawfully obtains or can lawfully obtain from the connected product or related service, without disproportionate effort going beyond a simple operation' (Art. 2 no. 17 DA).

[57] Pursuant to Art. 5 para. 1 DA, the data holder must make these data available 'to a third party without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge to the user, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time.'

[58] Art. 5 para. 3 and Art. 6 para. 2 lit. d DA.

[59] Art. 7 para. 1. Favorable rules are also provided for medium-sized enterprises by Art. 7 para. 1 subpara. 2 DA.

A further significant novelty[60] is that these new rights are linked to a set of presupposed obligations: First, designers and manufacturers of connected products and designers, as well as providers of related services, must make it possible that relevant data are, 'by default, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format, and, where relevant and technically feasible, directly accessible to the user.'[61] Second, those who sell, rent, or lease a connected product or provide related digital services must deliver the user 'in a clear and comprehensible manner' basic information on the data generated. The user must be given this information before the conclusion of the contract.[62]

If requested data are personal, coordination with the GDPR rules is required:[63] The first case to be examined is when the user is the natural person to whom the information to be shared relates. In such a case, the requesting user is a data subject according to the GDPR. From this perspective, the right introduced by the Data Act can be considered an enhanced right to data portability compared to the one set forth in Art. 20 GDPR.[64] If the personal data relates to individuals other than the user requesting the data sharing, the right to portability should be framed as a prerogative of an entity that, in the legal framework of the GDPR, qualifies as a data controller.[65] Since, from the perspective of the GDPR, these operations involving data are to be considered processing activities, they must be based on a legal ground that makes them lawful (Art. 6 and Art. 9 GDPR).[66] In any case, the third party receiving personal data from the data holder must comply with GDPR principles and obligations, including data subjects' rights.[67]

---

[60] *Wolters*, European Journal of Law and Technology 2024, Vol. 15 Iss. 1, 1 (16 et seq.).

[61] Art. 3 para. 1 DA.

[62] Art. 3 para. 2 and 3 DA. See *Wolters*, European Journal of Law and Technology 2024, Vol. 15 Iss. 1, 1 (16).

[63] GDPR primacy is affirmed by Art. 1 para. 5 DA. See *Chiarella/Borgese*, Athens Journal of Law 2024, Vol. 10 Iss. 1, 47 (59 et seq.).

[64] However, since direct access of the third party appointed by the user could require an agreement between the third party itself and the data holder, Art. 5 para. 8 DA states that 'Any failure on the part of the data holder and the third party to agree on arrangements for transmitting the data shall not hinder, prevent or interfere with the exercise of the rights of the data subject under Regulation (EU) 2016/679 and, in particular, with the right to data portability under Article 20 of that Regulation'. See also *Da Rosa Lazarotto*, European Journal of Law and Technology 2024, Vol. 15 Iss. 1, 1 (11).

[65] As a general rule, the right to share data cannot adversely affect data subjects' rights (Art. 5 para. 13 DA).

[66] Art. 4 para. 12 and Art. 5 para. 7 DA. The Data Act does not provide for a legal basis for the personal data processing: *Metzger*/*Schweitzer*, ZEuP 2023, Iss. 1, 42 (77). According to these Authors the interplay between the GDPR and the Data Act could hinder access requests. Despite the ambiguous wording, the rule requiring the legal basis refers specifically to the user or the third party designated by the user: *Wolters*, European Journal of Law and Technology 2024, Vol. 15 Iss. 1, 1 (20).

[67] Art. 6 para. 1 DA which further states that 'the third party shall erase the data when they are no longer necessary for the agreed purpose, unless otherwise agreed with the user in relation to non-personal data.'

## V. The EHDS Regulation Proposal: General Legal Framework

The last step forward of the right to data portability concerns electronic health data, which brings this right back to its traditional dimension of a tool in the hands of the data subject. This evolution refers to the Proposal for a European Regulation to establish a European health data space (EHDS).[68] The EU Commission had already announced the creation of this common data space in its Communication 'A European strategy for data'.[69] The aim is to foster individuals' control of their health electronic data and make them more accessible and transmissible within the EU.[70]

Within the EHDS context, health data can be personal or non-personal. When dealing with personal data, the applicable definition is given by Art. 4 para. 15 GDPR.[71] However, genetic data, defined separately in Art. 4 para. 13 GDPR,[72] are also included.[73] In the legal framework of the GDPR, these data belong to the special categories listed in Art. 9 para. 1 GDPR ('sensitive data'), with the consequence that the stricter rules laid down in Art. 9 para. 2 GDPR apply. By contrast, non-personal data can result from anonymous surveys or from anonymizing previously personal data.[74]

---

[68] EU Commission Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, Strasbourg, 3.5.2022, COM(2022) 197 final, 2022/0140 (COD). The European Parliament and the Council of EU reached on 14 March 2024 a Provisional Agreement, available at https://www.consilium.europa.eu/media/70909/st07553-en24.pdf (last accessed on: 17 July 2024). Below, references to legal provisions adopt the article numbering provided in the agreed text ('EHDS Agreed Text').

[69] *Supra*, fn. 21. Common data spaces are sectoral legal frameworks on data, which aim to strengthen the secure movement of information between people and organizations in relevant policy areas. The dual purpose is to remove technical and legal barriers and to increase stakeholders' confidence in the security and quality of data.

[70] According to Policy Programme 'Path to the Digital Decade' (Decision [EU] 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030, OJEU L 323/4, 19.12.2022), the 100 % of Union citizens should have access to their electronic health records by 2030.

[71] Health data are 'personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.' For example, health data can be information recorded by a health professional, data observed by a wearable device, or even data calculated by a wellness application.

[72] 'Genetic data' are 'personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.'

[73] Art. 2 para. 2 lit. a EHDS Agreed Text: 'Personal electronic health data' are 'data concerning health and genetic data as defined in Article 4 points (13) and (15), of Regulation (EU) 2016/679, processed in an electronic form.'

[74] Art. 2 para. 2 lit. b EHDS Agreed Text. Non-personal data are relevant for the secondary use (see *infra*) insofar as they are sufficient for the case relevant purpose. Recital 49 admits that state-of-the-art anonymization technology does not entirely prevent the risk of re-identification of the natural person to whom these data originally referred.

The proposed Regulation aims to provide some standard rules for the primary and secondary use of health data: 'Primary use' refers to the processing of data 'for the provision of healthcare to assess, maintain or restore the state of health of the natural person to whom that data relates, including the prescription, dispensation, and provision of medicinal products and medical devices, as well as for relevant social, administrative or reimbursement services.'[75] 'Secondary use' includes purposes other than the initial ones (such as the provision of healthcare according to their primary use) 'for which they were collected or produced.'[76] Legitimate secondary use purposes are listed in Art. 34 EHDS Agreed Text.[77] For both types of use, the EHDS Proposal specifies the legal basis for processing personal data in line with Art. 6 and 9 of the GDPR.[78]

Outlined rules on the secondary use of health electronic data are of utmost importance (Chapter IV). They aim to create a public governance system of health data in this field,[79] monitored by national health data access bodies (HDAB).[80] In short, data users may apply to access health data for secondary use. If the HDAB issues a data permit (Art. 46 EHDS Agreed Text) or grants a data request (Art. 47 EHDS Agreed Text), data holders are obliged to make health data available to the same body[81] (which will then provide them to the applicant according to the procedure established in Chapter IV). However, during the legislative process, attention increased to the protection needs of data subjects, who were finally granted an opt-out right.[82]

In Chapter III, the proposed EHDS Regulation lays down obligations concerning manufacturing, importing, and placing on the market of electronic health records (EHR) systems (Art. 13a et seqq.) as well as provisions regarding their technical aspects (Art. 23 et seqq.) and market surveillance (Art. 28 et seqq.). Further provisions are dictated for labeling wellness applications when they claim to be interoperable with an EHR system (Art. 31 et seqq.). However, wellness App interoperability does not entail that health data are directly transmitted to the EHR system since the shar-

---

[75] Art. 2 para. 2 lit. d EHDS Agreed Text.

[76] Art. 2 para. 2 lit. e EHDS Agreed Text.

[77] 'Purposes for which electronic health data can be processed for secondary use' include, for example, policy making and regulatory activities, official statistics, education and teaching activities and scientific research, development and innovation activities for products or services, training, testing and evaluating of algorithms (including in AI systems).

[78] See recitals 15 and 37 EHDS Agreed Text.

[79] *Rapisarda*, Sul costituendo spazio europeo dei dati sanitari, Responsabilità medica 2023, Iss. 4, 413 (420 et seq.).

[80] See *Quinn/Ellyne/Yao*, Computer Law & Security Review 2024, Vol. 54 article no. 105993, 1.

[81] Art. 41 EHDS Agreed Text. As recital 37 explains, this obligation is relevant as legal basis for the processing of personal data, in accordance with Art. 6 and Art. 9 GDPR.

[82] Art. 35f EHDS Agreed Text. On the discussion, cf. *Cimina*, The Proposal for a European Health Data Space: between pursued objectives and data protection challenges, ERA Forum 2023, Vol. 24 Iss. 3, 343 (355 et seqq.).

ing or transmitting of such data requires the consent of the natural person to whom they relate.[83]

The EU Commission is responsible for establishing and periodically updating a 'European electronic health record exchange format', which is intended to ensure full data accessibility and interoperability (Art. 6 EHDS Agreed Text).[84] In principle, the technical specifications developed by the Commission should be applicable at least for the priority categories of electronic health data for primary use, which are listed in Art. 5 EHDS Agreed Text.[85] This dataset refers to pre-established basic information that provides the essential picture of a natural person's health condition.[86] Accordingly, EHR systems must include a 'European interoperability component' (Art. 13a EHDS Agreed Text), which allows for receiving the priority data categories in the EHR exchange format.[87]

In the context of the primary use of electronic health data, healthcare professionals may have access to the health data of natural persons under their treatment (at least the priority categories listed in Art. 5 EHDS Agreed Text).[88] However, according to

---

[83] Art. 31a EHDS Agreed Text.

[84] Para. 1: 'Such format shall be commonly used, machine-readable and allow transmission of personal electronic health data between different software applications, devices and healthcare providers. The format should support transmission of structured and unstructured health data.'

[85] Para. 3: 'Member States shall ensure that the priority categories of personal electronic health data referred to in Article 5 are issued in the European electronic health record exchange format referred to in paragraph 1. Where such data are transmitted by automatic means for primary use the receiving provider shall accept the format of the data and be able to read it.'

[86] Such data include '(a) patient summaries; (b) electronic prescriptions; (c) electronic dispensations; (d) medical imaging studies and related imaging reports; (e) medical test results, including laboratory and other diagnostic results and related reports; (f) discharge reports'. According to Art. 5 para. 1 EHDS Agreed Text 'Member States may provide by virtue of national law that additional categories of personal electronic health data shall be accessed and exchanged for primary use pursuant to this Chapter'.

[87] Art. 2 para. 2 lit. nc EHDS Agreed Text. Cross-border exchange of health data for primary use will be supported by the already existing digital infrastructure MyHealth@EU that Member States will be obliged to join: Art. 12 and recitals 24–26 EHDS Agreed Text.

[88] Art. 7a EHDS Agreed Text. See also recital 15: 'As it is difficult to exhaustively determine in advance which data from the existing data in the priority categories are medically relevant in a specific episode of care, health professionals should have a wide access. In accessing data relating to their patients, health professionals should comply with the applicable law, codes of conduct, deontological guidelines or other provisions governing ethical conduct with respect to sharing or accessing information, particularly in life-threatening or extreme situations'. In several Member States, health data are already collected in health records, which have different objectives, including enabling health professionals to consult the necessary information about a patient's health in a timely manner (recital 5b EHDS Agreed Text). In Italy, the *Fascicolo Sanitario Elettronico* (FSE) was introduced by Decree-Law No. 179 of 18 October 2012, but its rules, amended many times, have been supplemented by several ministerial decrees (most recently ministerial decree 7 September 2023). Access by health professionals, except in cases of urgency, is still based on the patient's consent (Art. 8): cf. *Corso*, Il fascicolo sanitario elettronico 2.0. Spunti per una lettura critica, Nuove leggi civili commentate 2024, Iss. 2, 334 (354 et seqq.). Apart from that, the Italian framework already anticipates many of the novelties of the EHDS Regulation: for example, the right to restrict

the principle of data minimization, national law may specify what data can be accessed by specific healthcare professionals considering different healthcare tasks.[89]

Moreover, healthcare providers are obliged to register health data (at least 'data falling fully or partially' under the priority categories) processed for healthcare provision. They must also ensure that health data are always up-to-date.[90]

In line with the GDPR, the proposed Regulation specifies that processing relevant electronic health personal data does not require the data subject's consent in case of provision of healthcare.[91] However, the patient's will can prevail insofar as he or she exercises the right to restrict access to his or her personal data (Art. 8e EHDS Agreed Text) or to opt-out if Member States provide for such a right (Art. 8h EHDS Agreed Text).[92]

## VI. The Right to Access and the Right to Data Portability under the EHDS Proposal

Within the proposed EHDS Regulation, the first Section of Chapter II provides for rules concerning the 'Rights of natural persons in relation to the primary use of their personal electronic health data.'[93] Both the right to access personal data and the right to data portability are included. The rights of individuals under the EHDS legal framework are built upon the model of data subjects' rights under Art. 15 and 20 GDPR. The new provisions aim to 'specify' and 'supplement' these rights. However, they are restricted to a limited scope, namely to health data in primary use. Furthermore, to prevent new rules from leading to unexpected legal gaps to the detriment of individuals, the legal text finally opted to maintain a dual set of rights, which comple-

---

access ('*oscuramento*': Art. 9) and the right to enter information ('*taccuino personale*': Art. 5); see *Rapisarda*, Appunti sul fascicolo sanitario elettronico 2.0, Responsabilità medica 2024, Iss. 1, 57.

[89] Art. 7a para. 2 subpara. 2 EHDS Agreed Text.

[90] Art. 7 EHDS Agreed Text. Patients have the right to insert information in their own health record, provided that such information is clearly distinguishable from the data registered by health professionals (Art. 8b). They do not have the right to alter health data concerning them, but they can request rectification in accordance to Art. 16 GDPR (Art. 8c).

[91] Cf. *Rapisarda*, Responsabilità medica 2023, Iss. 4, 413 (417). Patient's consent is not required: See *EDPB-EDPS*, Joint Opinion 03/2022, on the Proposal for a Regulation on the European Health Data Space, 12 July 2022, m. n. 60, available at https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en (last accessed on: 17 July 2024). This conclusion was clearer in the rewording of Art. 4 para. 3 of the original Commission Proposal, as amended by the European Parliament, which referred to Art. 9 para. 2 lit. h GDPR. However, the same result can be gleaned through rules on the right to restrict access (see *infra*).

[92] In any case, safeguard mechanisms can be specified by Member State law, e. g. in case of emergency. The individuals' decision to opt-out in primary use must be reversible.

[93] The proposed Regulation confirms that these rights can be exercised on behalf of the data subject by persons authorised by the latter or his or her legal representatives, in accordance with national law rules: Cf. Art. 8a EHDS Agreed Text.

ment each other and are based on different legal grounds. In this sense, the rights of the EHDS Regulation complement, without replacing, those of the GDPR.[94] Accordingly, with regard to data access, individuals are entitled to invoke this right by basing their request on the legal framework of the EHDS Regulation or the one of the GDPR.[95]

The new right of access (Art. 8a EHDS Proposal) covers solely electronic health data.[96] Once data have been recorded in an EHR system, they must be immediately transmitted by the healthcare provider to the requesting individual. Such transmission must be 'free of charge and in an easily readable, consolidated, and accessible form.' These specifications make it clear that, unlike the corresponding right regulated by the GDPR,[97] data access is intended not only to inform the data subject but to make it possible for him or her to reuse his or her own data.[98] In this enhanced version, the right to access ends up overlapping with the basic version of data portability under Art. 20 para. 1 GDPR.[99] Indeed, patients and their representatives have the right to 'download an electronic copy, free of charge' of personal data (at least the priority ones) in the interoperable format of the European electronic health records and can transmit them to another data controller, without hindrance from the former controller.[100]

In its current version, the Proposed Regulation also expressly provides for the right of individuals to data portability.[101] This right is shaped on the direct portability model outlined in Art. 20 para. 2 GDPR. According to Art. 8d EHDS Agreed Text,

---

[94] Recital 6 EHDS Agreed Text.

[95] Recital 8 EHDS Agreed Text: 'The right of access to data by a natural person, established by Article 15 of Regulation (EU) 2016/679, should be further complemented in the health sector […]. Rights under Regulation (EU) 2016/679 should still apply, allowing individuals to benefit from the rights under both frameworks.'

[96] At least those that belong to the priority categories of electronic health data for primary use: Art. 8a EHDS Agreed Text.

[97] Cf. *Troiano*, in: Zorzi Galgano, Persona, 195 (198 et seq.).

[98] In the legal framework of the GDPR, the response to the data subject's access request can take up to one month (Art. 12 para. 3 GDPR: 'That period may be extended by two further months where necessary, taking into account the complexity and number of the requests'). In addition, the controller often transmits a hard copy or scanned documents to fulfill the data subject's request. This possibility can also be useful for the patient (and indeed the right to access under Art. 15 GDPR still applies). However, the new access right has a different purpose, that is the immediate data transmission, via an electronic health data access service. The underlying interest, then, is not only to make it less time-consuming for controllers to satisfy their request: See recital 8 EHDS Proposal.

[99] According to Art. 20 para. 1 GDPR data subjects have the right to retrieve their personal data in order to transmit them to another controller, without hindrance from the former controller.

[100] Art. 8a para. 2 EHDS Agreed Text. The right of access may be temporarily restricted, based on special reasons, especially ethical ones, at least until the first contract between the health care professional and the patient: Art. 8a para. 3 and recital 9 EHDS Agreed Text.

[101] The original text of the Proposal did not expressly mention the right to data portability. However, recitals were already clear in considering the right contained in Art. 3 para. 8 (in its original wording) as a form of right to data portability. See *Li/Quinn*, The European Health Data Space: An expanded right to data portability? Computer Law & Security Review 2024, Vol. 52 article no. 105913, 1 (2).

individuals can give access or request the healthcare provider to transmit their health data to other healthcare providers of their choice.[102]

Compared to general data portability under Art. 20 GDPR, this new right to portability has a limited subjective scope. The request can only be made to a healthcare provider. The data recipient must also qualify as a healthcare provider or an 'identified recipient in the social security or reimbursement services sector.'[103]

Due to the broad definition of health and healthcare, many entities fall under the scope of application of the new right. However, the fact that the request cannot be addressed to any health data holder confirms that the new portability right can only be exercised in the primary use context.[104] This means that data may be transmitted only for healthcare purposes, not other purposes, such as scientific research.

For cases not covered by this new right to data portability, general data portability under Art. 20 GDPR is still applicable. However, the new right is distinguished by significant improvements over the basic version under the GDPR.[105] First, the right can be exercised regardless of the legal basis under which the transmitting controller (the healthcare provider) collects, generates, or processes the patient's data.[106] Second, portable data includes even inferred data.[107] This is not surprising since patients' health often derives from inferences gleaned through other data (such as diagnostics, tests, and medical examinations[108]). Still, it represents a significant novelty compared to the other portability rights codified in the GDPR and subsequent legal acts. Third, while Art. 20 para. 2 GDPR specifies that the right to have data transmitted directly can be exercised only where it is 'technically feasible', Art. 8d EHDS

---

[102] This request must be fulfilled at least for data that fall into the priority categories listed in Art. 5: recital 11 EHDS Agreed Text.

[103] In the last case, 'such a transmission shall be one-way only' (Art. 8d para. 3 EHDS Agreed Text).

[104] Under the original wording of Art. 3 para. 8 of the EU Commission Proposal, the request recipient could have been any health data holder. Yet, in any case, the placement of the provision in the context of primary use already suggested that data portability was limited to that context. Cf. *Li/Quinn*, Computer Law & Security Review 2024, Vol. 52 article no. 105913, 1 (9 et seq.), who nevertheless endorsed the interpretation which extended the new portability right to secondary use.

[105] Limitations to data portability under the GDPR are set forth in Art. 20 para. 1 GDPR (see *Troiano*, in: Zorzi Galgano, Persona, 195 [211 et seqq.]): Data to be ported should be processed by the transmitting controller on the basis of consent or a contract and such processing should be carried out by automated means. Finally, the data subject can request only data that he or she has provided to the controller.

[106] Recital 6 EHDS Agreed Text: 'The rights and rules related to the primary use of personal electronic health data under Chapter II and III of this Regulation concern all categories of those data, irrespective of how they have been collected or who has provided them, of the legal ground for the processing under Regulation (EU) 2016/679 or the status of the controller as a public or private organization.'

[107] Recitals 5 and 12 EHDS Agreed Text. Under the GDPR, it is disputed whether 'provided data' also include observed data, but inferred data are indisputably outside the scope of the right to data portability (see *Troiano*, in: Zorzi Galgano, Persona, 195 [213 et seqq.]).

[108] Recital 5 EHDS Agreed Text.

Agreed Text takes this result for granted.[109] Technical feasibility must be ensured by the controller and the 'manufacturers of the systems used by the healthcare provider'.[110] Data transfer and access shall be immediate. The interoperability of data ported is guaranteed, even if the healthcare providers involved are located in different Member States, using the European electronic health record exchange format.[111] Individuals can ask for transmission in this format of health data that fall within the priority categories.[112] Data porting should be free of charge not only for the data subject but also for the recipient of the data, who cannot be asked for compensation.[113] Finally, it could be questioned whether the new version of the right to data portability outlined by Art. 8d EHDS Agreed Text further differs from the basic version of Art. 20 GDPR for covering personal and non-personal data.

The most convincing interpretation is that this new right to data portability should be limited to personal data, like the right enshrined in Art. 20 GDPR.[114] It is true that the Regulation concerns, in general, both personal and non-personal data. However, Art. 8d is laid down in the framework of individuals' rights over their health data, and it has a close connection with the right to access, which is expressly limited to personal electronic health data.[115] Furthermore, where the legislator has shaped a right for an individual to access and share non-personal data, such as in the Digital Markets Act and the Data Act, that extension of the right can be explained in a market logic, according to which individuals should take advantage of data they have contributed to generate. Such a logic is alien to the EHDS Regulation. The aim of enhancing individuals' control of their own data is to strengthen the right to health and its effectiveness.

## VII. Concluding Remarks

The post-GDPR evolution of the right to data portability goes toward overcoming the limitations and certain contradictions that characterise the original version of the right under Art. 20 GDPR. However, the strengthening of the right to data portability is not generalised but concerns specific areas, which can be identified in light of subjective criteria (e. g. the qualification in terms of gatekeeper or healthcare provider of the data controller) and objective criteria (e. g. the origin of the data from smart products or the health character of the information subject to the right).

---

[109] See *Li/Quinn*, Computer Law & Security Review 2024, Vol. 52 article no. 105913, 1 (10 et seq.); *Rapisarda*, Responsabilità medica 2023, Iss. 4, 413 (417).

[110] Art. 8d para. 1 EHDS Agreed Text.

[111] Art. 8d para. 2 EHDS Agreed Text.

[112] See Art. 8d para. 4 and Art. 6 para. 3 EHDS Agreed Text.

[113] Art. 9a EHDS Agreed Text.

[114] See also *Li/Quinn*, Computer Law & Security Review 2024, Vol. 52 article no. 105913, 1 (7 et seq.).

[115] Art. 8a EHDS Agreed Text.

The evolution of the right to data portability parallels the evolution of the European data market, which is based on the free and secure movement of data. This scenario results not only in the expansion of the right to data portability (which can also cover, for example, non-personal data) but also in the overlap between this right and other rights that have a broader subjective scope and content (e. g. the right to share IoT data). As a result, the data subject's position is strengthened when the content of the right that overlaps with data portability is his or her data. However, the autonomous character of these new rights should be stressed, revealing different interests underpinning data movement.

The evolution of data portability is justified by its frequently emphasised multifunctionalism. The potential of this right, created to give data subjects greater control over their personal data, has also quickly emerged as a powerful tool outside data protection rules, such as in the field of consumer protection and market regulation.

Data portability, however, benefits more than just the market. Even personality rights and society's collective interests, such as health, can profit from it.[116] The rights to access and portability of health data, as well as the fostering of movement in a secure environment of such data, is the cornerstone of the European regulation establishing an EHDS.

Finally, the most recent data legal instruments are characterised, compared to the GDPR, by focusing on the effectiveness of portability rights. On the one hand, these rights are formulated to ensure a practical outcome for those who exercise them; on the other hand, many efforts have been made concerning technical specifications and infrastructure that enable data interoperability.

[116] Data portability rights are key tools for increasing the individual's self-determination in the digital environment. For this reason, these rights are mentioned in the policy lines outlined in the 'European Declaration on Digital Rights and Principles for the Digital Decade', solemnly proclaimed by the European Parliament, the Council and the Commission on 15 December 2022 (2023/C 23/01).

# Macht in der digitalen Plattformökonomie

## Paradigmenwechsel in der Kartellrechtsdurchsetzung

*Rupprecht Podszun* und *Sarah Hinck*



## I. Einleitung

Als US-amerikanisches Importprodukt hat sich spätestens seit Mitte des 20. Jahrhunderts das Kartellrecht als wichtiges wirtschaftspolitisches Ordnungsinstrument zur Kontrolle und Abhilfe wirtschaftlicher Machtkonzentrationen in Europa etabliert. Etwas mehr als ein halbes Jahrhundert später sorgen erneut US-amerikanische Importe hierzulande dafür, dass an der Schlagkraft des Kartellrechts für genau diese Zielerreichung gezweifelt wird. Große Digitalkonzerne, allen voran die sogenannten GAFAM (Google, Apple, Facebook, Amazon und Microsoft), stellen aufgrund neuer

digitaler Geschäftsmodelle und den Herausforderungen der daraus entwickelten Plattformökonomie die Effektivität des Kartellrechts und dessen Durchsetzung auf den Prüfstand. Wellen erstarkter *Enforcements*, neue *Theories of Harm* und Rufe nach strukturellen Abhilfemaßnahmen gegen die *Big Tech*-Plattformen sind als globales Phänomen zu beobachten. Daneben entwickeln sich allerdings auch neue Regulierungstendenzen in Form von Plattformgesetzen, die das Kartellrecht komplementieren, allen voran der europäische Digital Markets Act (DMA).[1] Die Umsetzung des am 1.11.2022 in Kraft getretenen DMA zur Gewährleistung von Bestreitbarkeit und Fairness auf Plattformmärkten ist bereits im vollen Lauf. Gleichzeitig zeigen sich auch erste Durchsetzungsschwierigkeiten, insbesondere in Form von eingeleiteten *Non-Compliance* Verfahren der Kommission[2] und einem gerichtlichen Vorgehen der Adressaten gegen Kommissionsentscheidungen.[3] Die vielfach diskutierte Fragestellung, wie sich Macht digitaler Plattformen effektiv regulieren lässt, bleibt vor diesem Hintergrund von anhaltender Relevanz.[4]

Der Beitrag zeichnet die Evolution eines Paradigmenwechsels in der Kartellrechtsdurchsetzung nach. Hierfür werden Besonderheiten der digitalen Plattformökonomie beleuchtet und zur Begründung des Scheiterns der klassischen Kartellrechtsdurchsetzung herangezogen. Auf dieser Grundlage werden die verschiedenen Interventionsmodelle – Kartellrecht oder ex ante Regulierung – zur Bekämpfung der Marktmacht der Digitalkonzerne auf deutscher und europäischer Ebene dargestellt. Auf dieser Grundlage wird abschließend der Paradigmenwechsel der kartellrechtlichen Rechtsdurchsetzung hin zu einer Abkehr von dem großzügigeren Wirtschaftsliberalismus der letzten Jahrzehnte nachvollzogen.

---

[1] Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte), ABl. L 265/1 vom 12.10.2022.

[2] KOM, Entsch. v. 24.6.2024 – Fall DMA.100206 (Apple – new business terms); KOM, Entsch. v. 25.3.2024 – Fall DMA.100193 (Alphabet – Online Search Engine – Google Search – Art. 6[5]); KOM, Entsch. v. 25.3.2014 – Fall DMA.100185 (Apple – Operating System – iOS – Art. 6[3]); KOM, Entsch. v. 25.3.2024 – Fall DMA.100109 (Apple – Online Intermediation Services – app stores – App Store – Art. 5[4]); KOM, Entsch. v. 25.3.2024 – Fall DMA.100075 (Alphabet – Online Intermediation Services – app stores – Google Play – Art. 5[4]); KOM, Entsch. v. 25.3.2024 – Fall DMA.100055 (Meta – Art. 5[2]).

[3] EuG, Klage v. 16.11.2023 – Rs. T-1080/23 (Apple/Kommission); EuG, Klage v. 15.11.2023 – Rs. T-1078/23 (Meta Platforms/Kommission); EuG, Beschl. v. 9.2.2024 – Rs. T-1077/23 (Bytedance/Kommission).

[4] *Montjoye/Schweitzer/Crémer*, Competition Policy for the Digital Era. Final Report, 2019, abrufbar unter https://op.europa.eu/en/publication-detail/-/publication/21dc175c-7b76-11e9-9f05-01aa75ed71a1/language-en (Abrufdatum: 24.7.2024); *Bundesministerium für Wirtschaft und Energie*, Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft. Bericht der Kommission Wettbewerbsrecht 4.0, September 2019; *Podszun*, Empfiehlt sich eine stärkere Regulierung von Online-Plattformen und anderen Digitalunternehmen? in: Ständige Deputation des Deutschen Juristentages (Hrsg.), Verhandlungen des 73. Deutschen Juristentages. Hamburg 2020/Bonn 2022, Band 1: Gutachten/Teil F, 2020, 1.

## II. Besonderheiten und Auswirkungen der Plattformökonomie

Die GAFAM-Unternehmen befinden sich nun seit mehreren Jahren unangefochten an der Spitze der Listen mit den größten und wertvollsten Unternehmen der Welt mit astronomischer Marktkapitalisierung von bis zu 3.400 Mrd. US-Dollar.[5] Den Digitalkonzernen ist es erfolgreich gelungen, ihre Kernangebote (Google Suche, Amazon Marketplace, Apples iOS, das Windows Betriebssystem und Metas soziales Netzwerk Facebook) zu durchintegrierten, digitalen Ökosystem mit einer Vielzahl von miteinander verbundenen Produkten und Diensten auszubauen. Wer eine Online-Suche startet, spricht von „googeln"; wer eine Chat-Nachricht verschickt, schreibt eine „WhatsApp". Die Besonderheiten der Plattformökonomie liefern die ökonomischen Begründungen für die Erfolgsgeschichte der *Big Tech*-Plattformen. Geschäftsmodelle mehrseitiger Plattformen und die Bildung digitaler Ökosysteme begünstigen starke Monopolisierungstendenzen auf Basis von Datenvorteilen, Netzwerkeffekten und den damit verbundenen Skalierungseffekten, die die wirtschaftliche Machtkonzentration wiederum spiralartig steigern.[6]

### *1. Mehrseitige Plattformen als Bottleneck*

Die GAFAM vereint neben den technologiegetriebenen Geschäftsmodellen der Umstand, dass sie im Kern als mehrseitige Plattformen und daher als Vermittelnde (Intermediäre) oder Bottleneck zwischen Angebots- und Nachfrageseite agieren.[7] Digitale Plattformen lassen sich demnach als Marktplatz begreifen, auf dem Angebot und Nachfrage durch Algorithmen und Daten koordiniert werden, wodurch Such- und Transaktionskosten verringert werden. Anbietende können durch die Plattform viel mehr Nachfragende erreichen, und umgekehrt haben Nachfragende durch die Plattform eine Auswahl vieler verschiedener Anbietender.[8] Die Google Suche beispielsweise ist die Plattform, die Nutzer und Nutzerinnen und Anbietende von Webinhalten zusammenführt und dabei Werbung Dritter einspielt. Der Apple App Store ist die Plattform, die Nutzer und Nutzerinnen von Apple-Produkten und App-Entwicklern und Entwicklerinnen zusammenbringt. Ebenso können Nutzer und Nutzerinnen von Microsofts Betriebssystem Windows nur hierüber Softwareanwendungen nutzen. Amazon Marketplace und das soziale Netzwerk Facebook bringen ebenfalls Verbraucher und Verbraucherinnen und gewerbliche Nutzer und Nutzerinnen wie Werbetreibende oder Online-Händler und Online-Händlerinnen auf ihren Platt-

---

[5] Statista, Größte Unternehmen der Welt nach Marktkapitalisierung im Jahr 2024, Stand: 16.7. 2024, abrufbar unter https://de.statista.com/statistik/daten/studie/12108/umfrage/top-unternehmender-welt-nach-marktwert/ (Abrufdatum: 24.7.2024).

[6] Vgl. ErwGr. 2 DMA.

[7] *Rochet/Tirole*, Platform Competition in Two-Sided Markets, Journal of the European Economic Association 2003, Vol. 1 Iss. 4, 990; *Rochet/Tirole*, Two-sided markets: a progress report, The RAND Journal of Economics 2006, Vol. 37 Iss. 3, 645.

[8] *Podszun*, in: Ständige Deputation des Deutschen Juristentages, Verhandlungen, 1 (11).

formen zusammen. Die Mehrseitigkeit wirkt sich auch dadurch aus, dass Plattformen von verschiedenen Nutzergruppen unterschiedliche ökonomische, nicht zwingend monetäre, Gegenleistungen verlangen können.

Man unterscheidet transaktionsbezogene und zugangsbezogene Gegenleistungen.[9] Die Kehrseite der Mehrseitigkeit ist die Macht dieser Plattformen, wirtschaftliche Aktivitäten zu koordinieren und die Aktivitäten der Plattformnutzenden zu lenken. Intermediationsmacht aufgrund der Bottleneck-Position der Plattformen eröffnet verschiedene Steuerungs- und Auswahlmöglichkeiten. Gewerbliche Anbietende auf Plattformen verlieren die Hoheit über die Schnittstellen zu ihren Kunden und Kundinnen. Das „*Matchmaking*" zwischen Anbietenden und Nachfragenden findet auf der Plattformebene statt. Den Plattformen wächst dadurch auch eine Regelsetzungsmacht zu: Auf der Plattform ist nur das möglich, was nach den Spielregeln der Plattformbetreibenden passieren soll. Abgesichert wird dies schon durch die technischen Vorgaben und das Design, ggf. aber auch durch rechtliche Regelungen (z. B. in AGB). Das eröffnet mannigfaltige Einflussmöglichkeiten: Die Kommunikation gewerblicher Nutzer und Nutzerinnen mit ihren Endkunden und Endkundinnen kann gesteuert und kontrolliert werden, Daten können erfasst und ausgewertet werden oder das Design der *User Experience* kann einer gezielten Führung unterliegen. Oft ermöglicht dies auch eine Bevorzugung eigener Angebote der Plattformunternehmen in einem (vermeintlich fairen) Wettbewerb mit anderen Anbietenden auf der Plattform.[10]

### *2. Datenvorteile*

Datenvorteile spielen eine essenzielle Rolle bei den Geschäftsmodellen digitaler Plattformen. Daten, die von den gewerblichen Nutzenden der Plattform sowie den Konsumenten und Konsumentinnen generiert werden, werden regelmäßig von dem Plattformbetreibenden gesammelt, ausgewertet und verwertet. Die Datenanalytik erfolgt weitestgehend maschinell und versetzt die Plattformunternehmen in die Lage, Qualität und Funktionalität und vor allem Personalisierung ihrer Angebote stetig zu verbessern.[11] Diese Wertschöpfung aus den Daten der Nutzenden führt regelmäßig dazu, dass die Plattformnutzung und Dienste der Plattformunternehmen ohne weitere Entgeltleistung erfolgen. Nicht ohne Grund haben Bundeskartellamt und EuGH im Facebook-Fall die Datenverarbeitung in Internetgeschäftsmodellen als ein wettbewerblich hoch-relevantes unternehmerisches Verhalten eingestuft.[12] Digitale Plattformen schöpfen Vorteile aus den Daten, indem sie unmittelbaren Zugriff auf die von den Plattformnutzenden generierten Daten haben und diese aus unterschied-

---

[9] *Krämer*, in: Säcker/Bien/Meier-Beck/Montag (Hrsg.), Münchener Kommentar zum Wettbewerbsrecht I, 4. Aufl., 2023, Kap. 4, Rn. 41.

[10] Zur Berücksichtigung von Regelungssetzungsmacht von digitalen Plattformen siehe auch BKartA, Beschl. v. 5.7.2022 – Az. B2-55/21 – Rn. 417, 426 ff.

[11] *Urban*, Digitale Ökosysteme in der EU-Fusionskontrolle, NZKart 2024, 189 (190 f.).

[12] BKartA, Beschl. v. 6.2.2019 – Az. B6-22/16 (Facebook) – Rn. 482; EuGH, Urt. v. 4.7.2023 – Rs. C-252/21 (Meta Platforms u. a.) – Rn. 51.

lichen Quellen zusammenführen können. Dadurch sind die Plattformunternehmen in der Lage, Angebote gezielt auf Präferenzen und Bedürfnisse zuzuschneiden, die für wirtschaftliche Entscheidungen von Nutzern und Nutzerinnen von Bedeutung sind.[13] Daraus folgt, je mehr Nutzer und Nutzerinnen einer Plattform, desto mehr Daten werden aggregiert, wodurch Nutzerpräferenzen immer gezielter bestimmt werden können und letztendlich der Spiraleffekt des wirtschaftlichen Erfolges der Plattform immer weiter vergrößert wird. Gleichzeitig erhöht der exklusive Zugang der Plattformunternehmen zu großen Datenmengen – insbesondere im Zusammenhang mit Netzwerkeffekten – weiter die Marktzutrittsschranken für wettbewerbsfähige, monetarisierbare Alternativangebote.[14]

### *3. Netzwerkeffekte*

Netzwerkeffekte sind ein zentraler Erfolgsfaktor für die Machtkonzentration auf Plattformmärkten und können zu sogenannten „*Winner takes all*"-Märkten führen.[15] Betroffene Märkte werden gewonnen, wenn sie zugunsten eines Unternehmens „kippen" (*tipping*) und nur noch wenig Wettbewerb auf dem Markt stattfindet.[16] Hierbei stellen direkte und indirekte Netzwerkeffekte entscheidende Ursachen dar. Direkte (positive Netzwerkeffekte) zeichnen sich dadurch aus, dass der Wert der Plattform für die Nutzer und Nutzerinnen mit steigender Nutzerzahl ebenfalls steigt, wie es insbesondere bei sozialen Netzwerken oder geschlossenen Messengerdiensten der Fall ist. Indirekte Netzwerkeffekte sind hingegen dadurch charakterisiert, dass der Wert der Plattform mit steigenden Nutzerzahlen für die Marktgegenseite steigt.[17] Indirekte Netzwerkeffekte prägen beispielsweise die Attraktivität von App Stores: je größer die App-Auswahl für die Nutzer und Nutzerinnen im Store, desto attraktiver der App Store. Und umgekehrt, je mehr Nutzer und Nutzerinnen eine App durch einen App Store erreichen kann, desto attraktiver wird der App Store auch für die App-Anbietenden. Der Spiraleffekt des Plattformerfolgs durch Netzwerkeffekte liegt auf der Hand. Hinzu kommt, dass die aufgrund einer großen Nutzerzahl vorliegenden Größenvorteile geeignet sind, die bereits niedrigen Grenzkosten je weiteren Nutzenden weiter zu reduzieren.[18] Ohne relativierende Faktoren wie ein *Multihoming*-Verhalten oder Fluktuation der Nutzer und Nutzerinnen[19] wird wirksamer Wettbewerb infolge starker Netzwerkeffekte in der Plattformökonomie weitestgehend

---

[13] *Podszun*, in: Ständige Deputation des Deutschen Juristentages, Verhandlungen, 1 (14).

[14] BKartA, Beschl. v. 6.2.2019 – Az. B6-22/16 (Facebook) – Rn. 482.

[15] *Fletcher*, Digital Competition Policy: Are Ecosystems different? DAF/COMP/WD(2020)96, Rn. 10 f.

[16] *Fuchs*, in: Immenga/Mestmäcker (Hrsg.), Wettbewerbsrecht II, 7. Aufl., 2024, § 18 GWB Rn. 143.

[17] *Bien*, in: Säcker/Bien/Meier-Beck/Montag, MünchKommWettbR I, 4. Aufl., 2023, Art. 102 AEUV Rn. 258; *Podszun*, in: Ständige Deputation des Deutschen Juristentages, Verhandlungen, 1 (12).

[18] *Podszun*, in: Ständige Deputation des Deutschen Juristentages, Verhandlungen, 1 (12).

[19] *Fuchs*, in: Immenga/Mestmäcker, Wettbewerbsrecht II, 7. Aufl., 2024, § 18 GWB Rn. 144a.

ausgeschlossen und Marktpositionen werden weiter verfestigt. Für Anbietende wird zur Schlüsselfrage des Wettbewerbs, ob sie auf die Plattform kommen und wie sie dort gerankt werden. Sie verlieren den direkten Kontakt zu den Kunden und Kundinnen, die eigentlich die Schiedsrichter im Wettbewerb sein sollten.

### *4. Modulare Ökosysteme*

Eine weitere Gemeinsamkeit der GAFAM ist der Ökosystemcharakter ihrer Geschäftsmodelle, die aus einer Vielzahl konglomeratisch verbundener digitaler Produkte und Dienste bestehen. Apple verknüpft beispielsweise die Nutzung der Hardwareprodukte mit der Nutzung des Apple-eigenen Betriebssystems, dem App Store sowie dem integrierten virtuellen Assistenten Siri. Amazon-CEO *Jeff Bezos* selbst prägte in diesem Zusammenhang den Begriff des Amazon *Flywheels*. Von unterdurchschnittlich niedrigen Preisen angestoßen und durch große Nutzergruppen gewachsen ermöglicht der *Flywheel*-Effekt der Plattform, als Ökosystem stetig zu wachsen und sich immer weiter von Wettbewerbern abzusetzen.[20]

Konzeptionalisierungsansätze zur Begrifflichkeit des Ökosystems lehnen sich an den ökologischen Ursprung des Schlagworts an.[21] So umfasse ein Ökosystem einerseits die Biozönose als Beziehungsgefüge verschiedener Lebewesen untereinander und andererseits das Biotop als ihren Lebensraum. Die Parallelen der Biozönose in den digitalen Ökosystemen wird in dem Beziehungsgefüge aus vielen Akteuren auf der Plattform sowie der komplementären Produktarchitektur digitaler Plattformen gesehen. Das Biotop der digitalen Ökosysteme kann in der modularen Systemarchitektur gesehen werden, das sich dadurch von anderen Ökosystemen abgrenzt, indem es eine interne Interoperabilitätsstruktur vorgibt.[22]

Durch diese vernetzte, modulare Architektur verschiedener Produkte und Dienste der Plattform, die interoperabel sind und miteinander kommunizieren, werden zwar neue Effizienzen ermöglicht. Gleichzeitig wird eine Trennung von bislang separaten Produkten und Diensten durch diese fortschreitende Integration erschwert. Das führt letztendlich zu einer Verwischung der Abgrenzungsmöglichkeiten von Produktmärkten.[23] Auf Grund durchintegrierter, geschlossener Ökosysteme sind Nutzer und Nutzerinnen verleitet, diese Ökosysteme nicht zu verlassen, um alternative Angebote, sofern überhaupt interoperabel, wahrzunehmen (*Lock-in* Effekte). Die Vernetzung und Komplexität der Ökosysteme erschwert es zunehmend, die Machtposition der Plattformunternehmen zu durchbrechen. Die sich daraus ergebenden erheblichen erwirtschafteten finanziellen Ressourcen der Plattformunternehmen ermöglichen eine weitere Verfestigung der Machtpositionen durch weitergehende Unternehmens-

---

[20] Abrufbar unter: https://xsellco.com/resources/amazon-flywheel/ (Abrufdatum: 24.7.2024).

[21] *Van den Boom*, Regulating Competition in the Digital Network Industry: A Proposal for Progressive Network Industry, 2023, 152 ff.

[22] *Urban*, NZKart 2024, 189 (189 f.).

[23] *Podszun*, in: Ständige Deputation des Deutschen Juristentages, Verhandlungen, 1 (16 f.).

strategien. So können derart erfolgreiche Quasi-Monopolisten potentielle Wettbewerber aufkaufen oder von vornherein abschrecken (*killer acquisitions*, *kill zones*) und Geschäftsbereiche quersubventionieren.

## III. Defizite des Kartellrechts in der digitalen Plattformökonomie

In den USA als Kind der Industrialisierung und in Deutschland maßgeblich nach dem zweiten Weltkrieg durch die Pläne der Potsdamer Konferenz zur Demokratisierung der vermachteten deutschen Wirtschaft entstanden, wurde das Kartellrecht mit Blick auf die damals relevanten Industrien entworfen: Das deutsche und das europäische Kartellrecht sind die Rechtsgebiete für Kohle und Stahl. Kartellrechtliche Analyse- und Durchsetzungsinstrumente haben sich entsprechend anhand von klassischen Industriemärkten herausgebildet. Dieser Rechts- und Analyserahmen stößt in der Plattformökonomie im Hinblick auf digitale, mehrseitige Plattformen und Ökosystemstrukturen an seine Grenzen. Preisanalysen gestalten sich im Hinblick auf für Verbraucher und Verbraucherinnen oft kostenfreie, datenbasierte Geschäftsmodelle schwierig. Selbst Übertragungsversuche klassischer Fallgruppen wie der „*Essential Facility*"-Doktrin auf digitale Plattformen[24] helfen nicht über den Umstand hinweg, dass das Kartellrecht den Herausforderungen datenbasierter, zunehmend vernetzter Geschäftsmodelle nicht ausreichend gerecht wird. Typisierend lassen sich diese Schwächen des Kartellrechts vor allem durch die überlangen Verfahrensdauern, Schwächen der Marktabgrenzungen und herkömmlicher *Theories of Harm* zur Begründung von Wettbewerbsschäden, Schwierigkeiten adäquater Abhilfemaßnahmen sowie fragmentierten nationalen Lösungsansätze für grenzüberschreitende Geschäftsmodelle abbilden.

### *1. Problem Verfahrensdauer*

Die großen Kartellverfahren, die von der Europäischen Kommission oder dem Bundeskartellamt geführt wurden, werden immer wieder als Leuchtturmverfahren bezeichnet – sie werfen grundlegende Fragen der Wirtschaftsordnung auf und werden sorgfältig ökonomisch und juristisch analysiert. Kommt es zu Entscheidungen, werden diese mit ähnlicher Akribie von Gerichten überprüft. Doch die Sorgfalt hat einen Preis, nämlich die Verfahrensdauer. In der auf Geschwindigkeit und das rasche Kippen von Märkten angelegten Digitalökonomie wird das Verfahren zum Anachronismus. Es stellt inzwischen ein erhebliches Defizit bei der Durchsetzung des Kartellrechts dar.

---

[24] EuG, Urt. v. 10.11.2021 – Rs. T-612/17 (Google und Alphabet/Kommission) – Rn. 224; *Körber*, Konzeptionelle Erfassung digitaler Plattformen und adäquate Regulierungsstrategien, ZUM 2017, 93 (99).

Dabei spielt auch eine Rolle, dass die Behörden in Verfahren mit digitalen Unternehmen auf schier unendliche Ressourcen zur Rechtsverteidigung und kaum mehr zu bewältigende Datenmengen treffen. Der Intel-Fall der Kommission, in dem es um missbräuchliche Praktiken beim Vertrieb von Intel-Chips geht, ist fast 15 Jahre nach der Kommissionsentscheidung in der Sache immer noch nicht rechtskräftig vom Europäischen Gerichtshof entschieden.[25] Im Fall Google Shopping kam das Urteil des Gerichts der Europäischen Union rund sieben Jahre nach der Eröffnung des Verfahrens durch die Kommission im Jahr 2010.[26] Das Rechtsmittelverfahren vor dem Europäischen Gerichtshof ist noch anhängig.[27] Über die bahnbrechende Entscheidung des Bundeskartellamts gegen den Meta-Konzern, in der es erstmals einen Verstoß gegen das Missbrauchsverbot auf Grundlage eines Verstoßes gegen die DS-GVO begründet hatte und die durch zwei Eilverfahren und ein Vorabentscheidungsverfahren ging, ist acht Jahre nach Einleitung des Verfahrens immer noch nicht abschließend in der Hauptsache entschieden.[28]

Neben den erheblichen Ressourcen der betroffenen Unternehmen, teilweise asymmetrisch zu denen der Kartellbehörden, dürfte vor allem die verstärkte Berücksichtigung ökonomischer Analysen im Zuge des „*More Economic Approach*" zu einer erheblichen Verlängerung von Verfahren beigetragen haben. Die Möglichkeit von Effizienzeinreden in Kartellverfahren eröffnen Unternehmen die Möglichkeit, umfassend ökonomische Erkenntnisse zu etwaigen Effizienzvorteilen vorzutragen.[29] Überlange Verfahrensdauern schmälern die Zielerreichung des Kartellrechts erheblich: Weder werden zeitnah Wirkungen auf den Märkten erzielt, noch können Grundsatzfragen der Wirtschaftsordnung geklärt werden – zu groß ist gerade in digitalen Märkten die Entwicklungsdynamik.[30]

### *2. Inadäquate Marktabgrenzung*

Für die Kartellrechtsanwendung ist die Abgrenzung von Märkten zentral. In jedem größeren Fall wird genau bestimmt, welche Produkte und Dienste miteinander austauschbar sind und welche Wettbewerbsbeziehungen so bestehen. Die über Jahrzehnte gepflegte Abgrenzung von Märkten fällt dabei regelmäßig kleinteilig aus. Das

---

[25] KOM, Entsch. v. 13.5.2009 – Fall AT.37990 (Intel); das Verfahren ist beim EuGH als Rs. C-240/22 P (Kommission/Intel Corporation) und beim EuG als Rs. T-286/09 RENV (Intel Corporation/Kommission) anhängig.

[26] KOM, Entsch. v. 10.12.2010 – Fall AT.39740 (Google Search [Shopping]); EuG, Urt. v. 10.11.2021 – Rs. T-612/17 (Google und Alphabet/Kommission).

[27] EuGH, Rs. C-48/22 P (Google und Alphabet/Kommission).

[28] BKartA, Beschl. v. 6.2.2019, Az. B6-22/16 (Facebook); BGH, Beschl. v. 23.6.2020 – KVR 69/19 und Beschl. v. 8.3.2021 – KVR 96/20; OLG Düsseldorf, Beschl. v. 24.3.2021 – VI-Kart 2/19; EuGH, Urt. v. 4.7.2023 – Rs. C-252/21 (Meta Platforms u. a.).

[29] *Laitenberger/Kröger*, Towards an „even more efficient" approach? Reflections on the future of Regulation (EC) No 1/2003, ZEuP 2023, 621 (624); *Heinemann*, Competition law in need for speed, Concurrences 2021, Iss. 4, 2 (2).

[30] *Heinemann*, Concurrences 2021, Iss. 4, 2 (2).

Vorgehen bei der Marktabgrenzung ist zwar ein empirisch-analytisches, das aber nicht ohne normative Wertungen auskommt. Die Kartellbehörden gehen stets vom Produkt mit seinen qualitativen Eigenschaften aus.

Die Charakteristika der digitalen Plattformökonomie führen diese Art, Märkte zu definieren, an Grenzen. Die Digitalwirtschaft ist maßgeblich gekennzeichnet durch Vernetzung innerhalb der digitalen Ökosysteme. Diese Vernetzung liegt einerseits in Form von technisch integrierten, komplementären Produkten und Diensten der *Big Tech*-Unternehmen vor. Andererseits ist die Vernetzung durch die Sammlung und Nutzung generierter Daten über verschiedene Produkte und Dienste hinweg gegeben. Daten sind gerade die „Sprache", durch die ganz unterschiedliche Produkte und Leistungen miteinander vernetzt werden können. Am Beispiel des Autos lässt sich das gut erkennen: Früher war ein Auto ein in viele Einzelteile zerlegbares Industrieprodukt. Die Einzelteile konstituierten jeweils einen Markt – eine Stoßstange konnte nicht durch eine Kurbelwelle ersetzt werden. Das gilt heute zwar immer noch. Doch inzwischen sind sämtliche Einzelteile des Autos digital miteinander vernetzt, das Auto hat ein digitales Betriebssystem, an dem die Einzelteile angedockt sind. Einzelne Produktmärkte wachsen zusammen. In einer klassischen, kleinteiligen Produktmarkt-Abgrenzung kann das kaum mehr abgebildet werden.

Im Fusionsfall *Google/Fitbit* hat die Kommission beispielsweise 14 verschiedene relevante Märkte festgestellt.[31] Erste Ansätze für eine mögliche Überwindung dieser Schwierigkeiten finden sich in der überarbeiteten Bekanntmachung über die Abgrenzung des relevanten Marktes der Europäischen Kommission.[32] Die Kommission schlägt zwei Möglichkeiten vor. Zum einen können für digitale Ökosysteme bestehend aus einem primären Kernprodukt und damit verbundenen, mehreren digitalen Sekundärprodukten die Grundsätze zur Abgrenzung von Anschlussmärkten angewendet werden. Daneben können die Sekundärprodukte, wenn sie gebündelt angeboten werden, einen eigenen relevanten Markt bilden. Jedenfalls sind laut Bekanntmachung im Zusammenhang mit digitalen Ökosystemen ggf. Netzwerkeffekte, Wechselkosten und *Multihoming*-Entscheidungen bei der Marktabgrenzung zu berücksichtigen.[33] Ob diese Ansätze geeignet sind, die Schwächen der Marktabgrenzung bei der zutreffenden Abbildung der wirtschaftlichen Verhältnisse in der Plattformökonomie zu überwinden, bleibt anhand noch zu entwickelnder behördlicher und ggf. gerichtlicher Entscheidungspraxis abzuwarten. Das auf Märkten aufbauende und an Marktmacht anknüpfende Kartellrecht hat hier Schwierigkeiten.

---

[31] *Urban*, NZKart 2024, 189 (191) mit Verweis auf KOM, Entsch. v. 17.12.2020 – Fall M.9660 (Google/Fitbit) – Rn. 384.

[32] Mitteilung der Kommission, Bekanntmachung der Kommission über die Abgrenzung des relevanten Marktes im Sinne des Wettbewerbsrechts der Union (C/2024/1645), ABl. C 35/1 vom 22.2.2024.

[33] Ebd. Rn. 104.

*3. Fehlende Theories of Harm*

Allein in den Jahren 2000–2021 werden den GAFAM-Unternehmen 32 Unternehmenskäufe ab einem Wert von jeweils 1 Mrd. US-Dollar zugerechnet, angeführt von Microsoft mit insgesamt zwölf Akquisitionen.[34] Wettbewerbshüter auf der ganzen Welt haben in den letzten Jahrzehnten Transaktionen wie den Erwerb der Social Media-Plattform Instagram und des Messenger-Diensts WhatsApp durch Facebook mangels handfester Wettbewerbsbedenken erlaubt, sofern überhaupt die einschlägigen Prüfschwellen überschritten wurden.[35] Den Schwierigkeiten, solche Unternehmenszusammenschlüsse einer nachträglichen wettbewerbsrechtlichen Prüfung zu unterziehen, stellt sich aktuell die US-amerikanische Wettbewerbsbehörde auf Grundlage einer möglichen missbräuchlichen Erwerbsstrategie.[36] Als einer der Verursachungsfaktoren für das Nichteinschreiten der Wettbewerbshüter wird die Ungeeignetheit herkömmlicher *Theories of Harm* zur Erfassung von neuartigen Wettbewerbsgefahren gehandelt. Es fehlt weitgehend an etablierten Kriterien, wann in Fällen mit Digitalbezug eine Schädigung des Wettbewerbs vorliegt. Ein Beispiel: In langjähriger Fusionskontrollpraxis wurden nicht-horizontale Zusammenschlüsse nur selten als problematisch für den Wettbewerb erachtet.[37] Als kritisch galt es vor allem, wenn ein Wettbewerber aufgekauft wird. Dass es auch Unternehmen geben kann, die wie eine Spinne im Netz benachbarte Märkte durch Akquisitionen in ihr Netz ziehen, wurde übersehen und war bis zum Aufkommen der Digitalplattformen regelmäßig auch kein Thema. Klassische *Theories of Harm* und ihre Einteilung in horizontale, vertikale und konglomeratische Effekte werden den Wechselbeziehungen zwischen den verschiedenen Seiten digitaler Plattformen und der zu einem Ökosystem verbundenen Sytemarchitektur oftmals nicht gerecht.[38] Den seither entwickelten Ansätzen zur Überwindung dieser Durchsetzungslücke fehlt es bislang an Konkretisierung und Anwendungsfällen mit Präzedenzcharakter.[39] Verstärkt diskutiert werden in diesem Zusammenhang beispielweise Datenschutz-basierte, Innova-

---

[34] Abrufbar unter https://www.cbinsights.com/research/tech-giants-billion-dollar-acquisitions-infographic/ (Abrufdatum: 24.7.2024).

[35] Vgl. KOM, Entsch. v. 3.10.2014 – Fall M.7217 (Facebook/WhatsApp); OTF, Entsch. v. 14.8. 2012 – ME/5525/12 (Facebook/Instagram); FTC, Entsch. v. 22.8.2012 – Fallnr. 121 0121 (Facebook, Inc./Instagram, Inc.).

[36] FTC, Beschwerde v. 13.1.2021 – Case 1:20-cv-03590 (Federal Trade Commission v. Facebook, Inc.).

[37] *Urban*, NZKart 2024, 189 (189).

[38] OECD, Theories of Harm for Digital Mergers, OECD Competition Policy Roundtable Background Note, 2023, 25, abrufbar unter https://www.oecd-ilibrary.org/docserver/0099737e-en.pdf?expires=1721234034&id=id&accname=ocid195065&checksum=C041F64CBC6F7BC3D97B0252A9C939A (Abrufdatum: 24.7.2024).

[39] OECD, Theories of Harm for Digital Mergers, OECD Competition Policy Roundtable Background Note, 2023, abrufbar unter https://www.oecd-ilibrary.org/docserver/0099737e-en.pdf?expires=1721234034&id=id&accname=ocid195065&checksum=C041F64CBC6F7BC3D97B02520A9C939A (Abrufdatum: 24.7.2024).

tions-basierte und Ökosystem-basierte *Theories of Harm*.[40] Erschwert wurde die Bildung neuer Schadenstheorien durch große Vorsicht der Behörden gegenüber neuen Fallgruppen und ein Festhalten an ökonomischen Lehren, die die neuen Phänomene der Plattformökonomie noch nicht rezipiert hatten.

Eine Kehrtwende der Zurückhaltung stellt erst die 2023 erfolgte Untersagung im Zusammenschlussverfahren *Booking/eTraveli* dar, die die Europäische Kommission aussprach. In der Begründung der Wettbewerbsgefährdung führt die Kommission erstmals Aspekte einer Ökosystem-basierten Schadenstheorie an: Ohne eine Untersagung der Transaktion wäre das Hotelbuchungsportal Booking in der Lage gewesen, das eigene Reisebuchungs-Ökosystem weiter auszubauen und dadurch Netzwerkeffekte auf dem Kernmarkt zu stärken.[41] Was hier knapp für die Fusionskontrolle dargestellt wurde, gilt in ähnlicher Form für Kartell- und Missbrauchsverfahren. Die Etablierung der Fallgruppe der verbotenen Selbstbevorzugung etwa (*self-preferencing*) im Fall Google Shopping war heftig umstritten.[42]

### *4. Unzureichende Abhilfemaßnahmen*

Nicht nur die materielle Bewertung von Wettbewerbsgefahren auf digitalen Plattformmärkten durch stichfeste *Theories of Harm* bereitet Wettbewerbsbehörden und Gerichten bei der Rechtsdurchsetzung gegen digitale Plattformen Schwierigkeiten. Auch die Bestimmung adäquater Abhilfemaßnahmen hat sich als Herausforderung für die Kartellrechtsdurchsetzung bei der Ausräumung von Wettbewerbsbedenken erwiesen. Typischerweise beenden Wettbewerbsbehörden heute Verfahren nicht mehr bloß mit einer schlichten Untersagung. Vielmehr legen sie fest, welche Schritte unternommen werden müssen, um das wettbewerbliche Problem aufzulösen.

Besonders signifikant zeigte sich die Schwierigkeit, solche „*remedies*" zu designen, an der Odyssee im Google Shopping-Verfahren, in dem es mehr als ein Jahrzehnt in Anspruch genommen hat, geeignete Abhilfemaßnahmen zu finden. Ihre Wirksamkeit wird weiterhin in Zweifel gezogen.[43] Teilweise werden bei den Abhilfemaßnahmen kaum mehr überschaubare Überwachungszeiträume angesetzt: In der

---

[40] *Esayas*, Privacy as a Non-Price Competition Parameter: Theories of Harm in Mergers, University of Oslo Faculty of Law Research Paper No. 2018-26, 2018, abrufbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3232701 (Abrufdatum: 24.7.2024); OECD, Theories of Harm for Digital Mergers, OECD Competition Policy Roundtable Background Note, 2023, 31, abrufbar unter https://www.oecd-ilibrary.org/docserver/0099737e-en.pdf?expires=1721234034&id=id&accname=ocid195065&checksum=C041F64CBC6F7BC3D97B02520A9C939A (Abrufdatum: 24.7.2024); *Urban*, NZKart 2024, 189 (189).

[41] KOM, Entsch. v. 25.9.2023 – Fall M.10615 (Booking Holdings/eTravali Group) – Rn. 193.

[42] Zu den möglichen ökonomischen Vorteilen von Selbstbevorzugungspraktiken vgl. *Monopolkommission*, Sondergutachten 82, 2021, Rn. 91.

[43] KOM, Entsch. v. 27.6.2017 – Fall AT.39740 (Google Search [Shopping]); *Marsden*, Google Shopping for the Empress's New Clothes – When a Remedy Isn't a Remedy (and How to fix it), Journal of European Competition Law & Practice 2020, 553 (553 ff.); *Höppner*, Google's (Non-) Compliance with the EU Shopping Decision, 2020, abrufbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3700748 (Abrufdatum: 24.7.2024).

Freigabeentscheidung im Fusionskontrollfall *Google/Fitbit* wurde eine Laufzeit von zehn Jahren für die verhaltensbezogenen Zusicherungen mit entsprechendem Monitoring festgelegt.[44] Zweifel an der Wirksamkeit verhängter Abhilfemaßnahmen dürften letztendlich jedenfalls vor dem Hintergrund berechtigt sein, dass trotz mehr als 30 kartell- und fusionskontrollrechtlichen Verfahren der Europäischen Kommission gegen die GAFAM-Unternehmen in den letzten zehn Jahren[45] die digitalen Plattformkonzerne weitestgehend unbeirrt ihre Marktstellung weiter zementieren und sich von Wettbewerbern – sofern noch existent – weiter absetzen konnten.

*5. Erforderlichkeit harmonisierter Durchsetzungsergebnisse*

Trotz Unionsrechtsvorrangs wird die Kartellrechtsdurchsetzung in der EU auch maßgeblich von nationalen Wettbewerbsbehörden mitgetragen. So erlaubt Art. 3 VO (EG) Nr. 1/2003 materiell-rechtlich den Mitgliedstaaten ausdrücklich strengere Maßnahmen für einseitige Handlungen von Unternehmen. Die Verordnung regelt auf prozessualer Seite weiter die komplexe Zusammenarbeit zwischen der Europäischen Kommission und den nationalen Wettbewerbsbehörden. Nicht nur aufgrund der zum Teil dezentralen Durchsetzung des Kartellrechts im europäischen Binnenmarkt fehlt es angesichts der grenzüberschreitenden Geschäftsmodelle der Digitalkonzerne trotz Leitentscheidungen der Europäischen Kommission bisweilen an einer europaweit einheitlichen Durchsetzungspraxis. In dem bahnbrechenden Flaggschiffverfahren des Bundeskartellamts gegen den Meta-Konzern und dessen Datennutzungspraxis wurden beispielsweise allein die Vorschrift des deutschen Missbrauchsverbots herangezogen, nicht des europäischen.[46] Im Kampf gegen Apples *Anti-Steering* Klauseln akzeptierte die niederländische Wettbewerbsbehörde Zusicherungen allein für iOS Dating Apps in den Niederlanden.[47] Mehr als drei Jahre später traf die Europäische Kommission eine ähnliche Entscheidung nur betreffend Musik Streaming-Apps wie Spotify in der EU auf Apples iOS-Geräten.[48] Auch die Beurteilung der Kartellrechtswidrigkeit von Preisparitätsklauseln digitaler Plattformen war Gegenstand unterschiedlicher Entscheidungspraxis in den Mitgliedstaaten.[49] Spätestens mit der Einführung des § 19a GWB, einer spezifischen nationalen Regelung für Wettbewerbsbehinderungen durch Unternehmen mit marktübergreifend überragen-

---

[44] KOM, Entsch. v. 17.12.2020 – Fall M.9660 (Google/Fitbit).

[45] Vgl. Auswertung der Fusionskontrollfälle in der Entscheidungsdatenbank der Kommission, abrufbar unter https://competition-cases.ec.europa.eu/search?sortField=caseLastDecisionDate&sortOrder=DESC (Abrufdatum: 24.7.2024).

[46] BKartA, Beschl. v. 6.2.2019, Az. B6-22/16 (Facebook).

[47] ACM, Fallbericht v. 24.1.2021 – Fallnr. ACM/19/035630.

[48] KOM, Entsch. v. 6.5.2024 – Fall AT.40437 (Apple – App Store Practices [music streaming]).

[49] Zusammenfassend vgl. *Augenhofer/Schwarzkopf*, Bestpreisklauseln im Spannungsfeld europäischen Kartellrechts und mitgliedstaatlicher Lösungen, NZKart 2017, 446; BGH, Beschl. v. 14.7.2020 – KVZ 56/19; siehe dazu *Kühling/Ceni-Hulek/Engelbracht*, Alles wieder auf Anfang – Zur kartellrechtlichen Bewertung enger Bestpreisklauseln auf Hotelportalen, NZKart 2021, 76.

der Macht, dürfte die drohende Fragmentierung der kartellrechtlichen Durchsetzung im Digitalbereich auf der Hand gelegen haben.

## IV. Interventionsmodelle – Kartellrecht vs. Regulierung

Die Grenzen des Kartellrechts als Regulierungsinstrument zur Begrenzung wirtschaftlicher Macht digitaler Plattformen haben zur verstärkten Debatte um die Leistungsfähigkeit des Kartellrechts und letztlich zu einer Reihe von Reformen auf Gesetzgebungsebene geführt. Ist das Kartellrecht noch in der Lage, den Wettbewerb und damit das Funktionieren der Marktwirtschaft im digitalen Zeitalter zu schützen? Der Blick auf die ökonomische Wirklichkeit zeigt, dass der Kampf für freien Wettbewerb im Netz beinahe verloren ist. Einige wenige Anbietende stellen die Infrastruktur der Digitalwirtschaft zur Verfügung und können in immer weiteren Bereichen ihre Macht ausdehnen und andere Unternehmen in Abhängigkeitsszenarien bringen. Selbst die europäische Automobilwirtschaft, einst der Stolz des Kontinents, kooperiert inzwischen mit Diensten wie Google und Amazon für das automobile Betriebssystem. Wer in diesen Konstellationen am Steuer sitzt und wer nur noch Beifahrer oder Beifahrerin ist, ist nicht ausgemacht. Abgesehen von dem hier mitschwingenden industriepolitischen Lamento ist aber vor allem die Wettbewerbslage prekär: Digital erfolgreich zu sein, geht nur noch zu den von den GAFAM gesetzten Bedingungen.

Das haben auch die gesetzgebenden Institutionen erkannt und nachgesteuert. In Deutschland hat das Kartellrecht ein Update zur besseren Erfassung von Wettbewerbsgefahren auf digitalen Plattformmärkten erhalten. Auf europäischer Ebene trat der DMA als Regulierungsgesetz und Nicht-Kartellrecht in Kraft. Andere Jurisdiktionen scheinen zu folgen.[50] Die gewählten Ansätze unterscheiden sich jedoch in der Wahl des Regulierungsinstruments zwischen einer Reform oder stärkeren Durchsetzung des Kartellrechts[51] oder neuen, das Kartellrecht komplementierenden Gesetzen.[52] Die Diskrepanzen zwischen (Sonder-)Kartellrecht einerseits und neuen Regulierungsgesetzen andererseits als neue Interventionsmodelle lassen sich anhand der Darstellung der Änderungen des deutschen Kartellrechts durch die letzte GWB-Novelle, allen voran der Einführung des § 19a GWB, sowie des DMA aufzeigen.

---

[50] Für Legislativvorhaben bspw. in der Türkei siehe https://www.csis.org/analysis/turkey-considering-new-digital-competition-legislation (Abrufdatum: 24.7.2024), in Brasilien siehe https://www.csis.org/analysis/brazil-considering-new-digital-competition-legislation (Abrufdatum: 24.7.2024).

[51] So verfolgen laufende Kartellverfahren in den USA beispielsweise das Ziel struktureller Abhilfemaßnahmen in Form von Unternehmensentflechtungen, vgl. US Department of Justice, Beschwerde v. 24.1.2024 – Case 1:23-cv-00108 (United States of America u. a. v. Google LLC); FTC, Beschwerde v. 19.8.2021 – Case 1:20-cv-03590-JEB (Federal Trade Commission v. Facebook, Inc.).

[52] Vgl. Inkrafttreten des *Digital Markets Competition and Consumer Acts* in Großbritannien am 24.5.2024, abrufbar unter https://bills.parliament.uk/bills/3453 (Abrufdatum: 24.7.2024).

*1. Update für das deutsche Kartellrecht: Das GWB-Digitalisierungsgesetz*

Das GWB-Digitalisierungsgesetz wurde im Januar 2021 vom deutschen Bundestag verabschiedet. Im internationalen Diskurs um die legislativen Möglichkeiten, die Macht von digitalen Plattformen einzudämmen, hat diese 10. GWB-Novelle eine Vorreiterrolle eingenommen. Ähnliche Reformen wurden daraufhin auch auf europäischer Ebene vorgeschlagen.[53] Der deutsche Gesetzgeber setzte damit weiterhin auf Kartellrecht. Auch wenn der neu eingeführte § 19a GWB Nähe zum Regulierungsrecht aufweist, handelt es sich als „besondere Missbrauchsaufsicht" um eine kartellrechtliche Vorschrift.[54]

*a) Vorreiterrolle des § 19a GWB*

Im Kern der 10. GWB-Novelle steht die Einführung des § 19a GWB. Als kartellrechtliche Vorschrift bezweckt § 19a GWB weiterhin den Schutz des Leistungswettbewerbs angesichts der erheblichen Konzentration von Macht in der Plattformökonomie durch digitale Ökosysteme.

Die Vorschrift ist auf einen engen Adressatenkreis zugeschnitten und folgt einem zweistufigen Aufbau.

Nach § 19a Abs. 1 GWB kann die deutsche Wettbewerbsbehörde, das Bundekartellamt, die überragende, marktübergreifende Bedeutung eines Unternehmens für den Wettbewerb per Verfügung feststellen. Die Anknüpfung an eine überragende, marktübergreifende Bedeutung stellt eine Abkehr von der traditionellen Marktabgrenzung dar.[55] Dabei muss das Unternehmen in erheblichem Umfang auf mehrseitigen Märkten oder in Netzwerken tätig sein. Bei der Feststellungsentscheidung zu beurteilende Faktoren sind in § 19a Abs. 1 S. 2 Nr. 1–5 GWB gelistet und beziehen sich beispielsweise auf Indikatoren wie Marktbeherrschung, Finanzkraft, Zugang zu wettbewerbsrelevanten Daten oder vertikale oder anderweitig integrierte Tätigkeiten auf unterschiedlichen Märkten.

Die Feststellungsverfügung aus § 19a Abs. 1 GWB ist konstitutiv für das Auslösen des Verbotskatalogs aus § 19a Abs. 2 GWB. Allerdings werden die Verbote aus Abs. 2 nicht automatisch durch die Feststellungsverfügung nach Abs. 1 aktiviert. Vielmehr bedarf es eines gesonderten Verfahrens mit abschließender Verbotsverfügung durch das Bundeskartellamt. Ziel der Verbotstatbestände des § 19a Abs. 2 GWB ist die Begrenzung wirtschaftlicher Macht sowie die Offenhaltung von Märkten für andere Akteure.[56] § 19a Abs. 2 S. 1 GWB enthält sieben Verbotstatbestände, die abschließend sind, gleichzeitig jedoch eine flexible Handhabung durch eine Kon-

---

[53] *Bundesministerium für Wirtschaft und Energie*, Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft. Bericht der Kommission Wettbewerbsrecht 4.0, 2019.

[54] *Schweitzer*, in: Immenga/Mestmäcker, Wettbewerbsrecht II, 7. Aufl., 2024, § 19a GWB Rn. 43; *Wolf*, in: Säcker/Bien/Meier-Beck/Montag, MünchKommWettbR I, 4. Aufl., 2023, § 19a GWB Rn. 4.

[55] *Schweitzer*, in: Immenga/Mestmäcker, Wettbewerbsrecht II, 7. Aufl., 2024, § 19a GWB Rn. 94.

[56] BegrRegE 10. GWB-Novelle, BT-Drs. 19/23492, 75, 77.

kretisierung durch Regelbeispiele mit Indizwirkung erlauben. Die Verbotstatbestände sind nicht rein prophylaktisch, sondern erfordern eine Wettbewerbsgefährdung, soweit diese im Tatbestand angelegt ist. Ein tatsächlich eingetretener Wettbewerbsschaden ist jedoch nicht erforderlich.[57] Materiell-rechtlich untersagen die Verbotstatbestände den nach § 19a Abs. 1 GWB bestimmten Unternehmen verschiedene Praktiken, darunter Selbstbevorzugung (Nr. 1), Behinderung auf Absatz- und Beschaffungsmärkten, z. B. durch Vorinstallation eigener Angebote (Nr. 2), oder Behinderung anderer Unternehmen durch Datenverarbeitung (Nr. 4).

Ausfluss der kartellrechtlichen Prägung der Vorschrift ist auch die Möglichkeit der sachlichen Rechtfertigung nach § 19 Abs. 2 S. 2 GWB, die eine Rechtfertigung der Adressaten durch den Vortrag von Effizienzerwägungen erlaubt.

Ein wesentlicher Zweck des § 19a GWB ist die Überwindung der überlangen Verfahrensdauern der Missbrauchsfälle und damit die Verfahrensbeschleunigung. Dazu dient zum einen die konstitutive Feststellungsverfügung nach § 19a Abs. 1 GWB. Daneben wird jedoch auch prozessual eine Beschleunigung durch die Verkürzung des Rechtswegs erreicht. Nach § 73 Abs. 5 GWB gehen Beschwerden gegen Entscheidungen des Bundeskartellamts unter Anwendung von § 19a GWB in erster und letzter Instanz an den Bundesgerichtshof. Inwieweit sich die erwünschte Beschleunigung auch bei Durchsetzung der in § 19a Abs. 2 GWB spezifizierten Verbote erreichen lässt, bleibt abzuwarten. Seit Januar 2021 hat das Bundeskartellamt bereits sieben Verfahren auf Grundlage der erweiterten Missbrauchsaufsicht gemäß § 19a Abs. 2 GWB eingeleitet und davon erst zwei Verfahren abgeschlossen.[58]

*b) Weitere Updates für das deutsche Wettbewerbsrecht*

Die Einführung des § 19a GWB in das deutsche Wettbewerbsrecht wird ergänzt durch weitere Reformen im Zuge der letzten GWB-Novellen zur besseren Erfassung von Wettbewerbsgefahren auf digitalen Plattformmärkten.

Auch als Reaktion auf sogenannte *Killer Acquisitions* und insbesondere den Zusammenschluss Facebook/WhatsApp, der die Umsatzschwellen für eine Anmeldepflicht des Zusammenschlusses überschritt, wurde bereits 2017 mit der 9. GWB-Novelle die Transaktionsschwelle in das deutsche Fusionskontrollrecht eingeführt.[59] Nach § 35 Abs. 1a GWB können nun auch Transaktionen erfasst werden, die einen Transaktionswert von mehr als 400 Mio. Euro erzielen, wenn das Zielunternehmen „in erheblichen Umfang im Inland tätig ist".[60]

---

[57] *Wolf*, in: Säcker/Bien/Meier-Beck/Montag, MünchKommWettbR I, 4. Aufl., 2023, § 19a GWB Rn. 35.

[58] BKartA, Laufende Verfahren gegen Digitalkonzerne (Stand 07/24), abrufbar unter https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Downloads/Liste_Verfahren_Digitalkonzerne.html?nn=50118 (Abrufdatum: 24.7.2024).

[59] RegE 9. GWB-Novelle, BT-Drs. 18/10207, 70–72.

[60] Zur Auslegung der Voraussetzung siehe OLG Düsseldorf, Beschl. v. 23.11.2022 – 3 Kart 119/21 (V) (Meta/Kustomer).

Der besseren Erfassung von Marktverhältnissen auf digitalen Plattformmärkten diente auch die Einführung von § 18 Abs. 2a und Abs. 3a GWB, die schon mit der 9. GWB-Novelle ergänzt worden waren. Klarstellend wurde für die Bestimmung von Marktbeherrschung ergänzt, dass es der Annahme von Märkten nicht entgegensteht, wenn Leistungen unentgeltlich erbracht werden. Zur Bewertung von Marktstellungen bei mehrseitigen Märkten und Netzwerken sind zudem Faktoren wie Netzwerkeffekte, *Multihoming* und Wechselaufwand von Nutzern, Zugang zu wettbewerbsrelevanten Daten sowie innovationsgetriebener Wettbewerbsdruck zu berücksichtigen.

Mit der 10. GWB-Novelle hat das deutsche Wettbewerbsgesetz auch erstmals eine *Anti-Tipping*-Regel erhalten. Mit der Einführung des § 20 Abs. 3a GWB hat die Gesetzgebung einen Eingriffstatbestand für Unternehmen mit relativer oder überlegener Marktmacht im Sinne der Vorschrift geschaffen, um zu verhindern, dass ein durch starke positive Netzwerkeffekte geprägter Markt zu einem monopolistischen Markt kippt.[61] Gleichzeitig wurden kartellrechtliche Regeln zur Berücksichtigung von erheblichen Datenvorteilen geschaffen. Relative oder überlegene Marktmacht gem. § 20 Abs. 1a GWB kann sich auch aus der Abhängigkeit von Datenzugängen ergeben. Zudem kann ein Missbrauch einer marktbeherrschenden Stellung auch bei Zugangsverweigerung zu Daten vorliegen (§ 19 Abs. 2 Nr. 4 GWB).[62]

Ohne den Pfad des Kartellrechts zu verlassen, hat die deutsche Legislative damit früh auf die Besonderheiten der digitalen Plattformökonomie reagiert und parallele Entwicklungen auf EU-Ebene angestoßen.

### *2. Regulierung: Der Digital Markets Act als neues Interventionsmodell*

Auf europäischer Ebene haben sich die gesetzgebenden Institutionen allerdings bewusst gegen eine mögliche Anpassung des EU-Kartellrechts entschieden und stattdessen einen Regulierungsakt eingeführt, den Digital Markets Act (DMA). Das neue Durchsetzungsmodell des DMA wird nachfolgend in seinen Grundzügen skizziert. Auch wenn viele Elemente aus dem Kartellrecht übernommen wurden, darunter auch Parallelen zu § 19a GWB, weist die Durchsetzungssystematik des DMA signifikante Neuerungen auf.

#### *a) Konstitutive Torwächterbenennung*

Ähnlich wie § 19a GWB, sieht auch der DMA ein zweistufiges Verfahren vor, in dem die Einstufung als Gatekeeper (Torwächter) in einem ersten Schritt nach Art. 3 DMA konstitutiv ist für das Auslösen der Verpflichtungen in Art. 5–7, 14, 15 DMA. Die Benennungsentscheidung löst diese Verpflichtungen automatisch aus, eines geson-

[61] BegrRegE 10. GWB-Novelle, BT-Drs. 19/23492, 82; vgl. auch *Stancke*, in Bunte/Stancke (Hrsg.), Kartellrecht. mit Vergaberecht und Beihilfenrecht, 4. Aufl., 2022, Rn. 165.

[62] BegrRegE 10. GWB-Novelle, BT-Drs. 19/23492, 72.

derten Verfahrens bedarf es nicht: Wer Torwächter ist und zentrale Plattformdienste (ZPD) betreibt, unterliegt einer Vielzahl neuer Pflichten.

Die Einstufung als Torwächter ist mehrgliedrig aufgebaut. Ausgangspunkt sind die in Art. 3 Abs. 1 DMA genannten qualitativen Kriterien, deren Erfüllung beim Vorliegen bestimmter quantitativer Kriterien (Nutzerzahlen und Marktkapitalisierung) in Art. 3 Abs. 2 DMA vermutet wird. Ähnlich wie bei § 19a GWB dient die stark formalisierte Normarchitektur einem Verzicht auf zeitintensive Feststellungen und Einzelfallanalysen sowie ggf. ökonomischer Analysen von Marktbeherrschung.[63] Die Torwächterbenennung wird aber flexibilisiert durch die Möglichkeit der Widerlegung der Vermutungsregel aufgrund quantitativer Schwellenwerte in Art. 3 Abs. 5 DMA. Um dem Beschleunigungszweck dennoch gerecht zu werden, unterwirft der DMA das Widerlegungsverfahren engen, von der Kommission einzuhaltenden Entscheidungsfristen. Die Anknüpfung an (relativ) einfach zu bestimmende Kennzahlen für die Designation als Torwächter ist weit entfernt von der Marktmachtschwelle im kartellrechtlichen Missbrauchsverbot.

Für die Torwächterbenennung nach Art. 3 DMA ist es erforderlich, dass der potentielle Torwächter mindestens einen ZPD anbietet. Die ZPD sind in einer abschließenden und bindenden Liste in Art. 2 Nr. 2 DMA angeführt.[64] Damit wird der Anwendungsbereich des DMA verbindlich festgelegt. Für die Aufnahme weiterer ZPD in den DMA kann die Kommission eine Marktuntersuchung durchführen, eine Ergänzung des Art. 2 Nr. 2 DMA ist dann jedoch nur im Wege eines Gesetzgebungsverfahrens möglich (vgl. Art. 19 Abs. 1, Abs. 3 lit. a DMA).

*b) Verhaltenspflichten als self-executing rules*

Kernstück des DMA ist die gesetzliche Ausgestaltung der Verpflichtungen in Art. 5–7 DMA als „*self-executing rules*“, die automatisch sechs Monate nach der Benennungsentscheidung des Torwächters für jeden ZPD einzuhalten sind. Der Unterschied zwischen Art. 5 DMA einerseits und Art. 6 und 7 DMA andererseits besteht darin, dass nur für Art. 6 und 7 DMA ein sogenanntes Spezifizierungsverfahren nach Art. 8 Abs. 2, 3 DMA vorgesehen ist. In diesem kann die Kommission Hinweise zur rechtskonformen Umsetzung der Verpflichtungen, die eigentlich aus sich heraus gelten sollen, geben. Die Verpflichtungen sind in der Verordnung sehr detailliert und präzise formuliert – es soll (anders als im stärker generalklauselartigen Kartellrecht) jeder Rechtsunterworfene nach der Lektüre wissen, was zu tun ist.

Im Hinblick auf ihren inhaltlichen Regelungsgehalt kann eine Einteilung der Verpflichtungen aus Art. 5–7 DMA in vier Kategorien vorgenommen werden: (i) Verpflichtungen in Bezug auf mögliche Datenvorteile,[65] (ii) Interoperabilitäts- und Zu-

[63] *Käseberg/Gappa*, in: Podszun (Hrsg.), Digital Markets Act. Gesetz über digitale Märkte, 2023, Art. 3 DMA Rn. 2.

[64] *König*, in: Säcker/Bien/Meier-Beck/Montag, MünchKommWettbR I, 4. Aufl., 2023, Art. 2 DMA Rn. 10.

[65] Art. 5 Abs. 2, 9, 10; Art. 6 Abs. 2, 8, 9, 10, 11 DMA.

gangsvorschriften,[66] (iii) Verbot von *Anti-Steering* und Selbstbevorzugungs-Praktiken[67] sowie (iv) sonstige Verpflichtungen von allgemeinerem, prozessualem Charakter.[68] Viele der Verpflichtungen in Art. 5 und 6 DMA finden ihren Ursprung in kartellrechtlichen Verfahren.[69] Das Verbot der Datenzusammenführung und -nutzung ohne qualifizierte Einwilligung in Art. 5 Abs. 2 DMA beruht beispielsweise maßgeblich auf dem kartellrechtlichen Verfahren des Bundeskartellamts gegen Metas Datenzusammenführungspraktiken.[70] Das Verbot der Selbstbevorzugung eigener Angebote aus Art. 6 Abs. 5 DMA ist maßgeblich vom *Google Shopping*-Fall der Kommission inspiriert.[71] Was als Grundsatzentscheidung im Kartellrecht begann, wird hier aber als regulatorische Vorgabe verallgemeinert. Effizienzeinwände können von den Torwächtern nicht vorgebracht werden. Trotz Anlehnung an kartellrechtliche Verfahren sind die Verpflichtungen eigenständig im Hinblick auf die Ziele des DMA auszulegen, nämlich Bestreitbarkeit und Fairness auf Märkten zu sichern.[72] Neben den Verpflichtungen aus Art. 5–7 DMA enthält Art. 14 DMA die Verpflichtung für Torwächter, die Kommission über jegliche Zusammenschlüsse im Sinne der Verordnung (EG) Nr. 139/2004 zu unterrichten. Von einer materiell-rechtlichen Regelung zur Beurteilung von Torwächter-Zusammenschlüssen wurde hingegen abgesehen.

### *c) Reduziertes Verfahrensrecht, Marktuntersuchungen und strukturelle Abhilfemaßnahmen*

In verfahrensrechtlicher Hinsicht weicht der DMA stark vom kartellrechtlichen Durchsetzungsregime ab. Insbesondere wurde im DMA von einem Rückgriff auf kartellrechtliche Verfahrensregeln abgesehen, das DMA-Verfahrensrecht in Art. 20–40 DMA eher kurz gehalten und die Durchsetzung an allen Stellen mit engen Fristen versehen. Ein formales Beteiligungsrecht für Dritte an den Verfahren sieht der DMA nicht vor.[73] Vielmehr beschränkt sich die Rolle Dritter auf Möglichkeiten zur Abgabe von Stellungnahmen in bestimmten Fällen. Auch hierin dürfte sich der dem DMA zugrundeliegende Beschleunigungsgedanke wiederfinden. Neben der Einleitung des Nicht-Einhaltungsverfahrens nach Art. 20 DMA wegen möglicher Verstöße gegen die Verpflichtungen aus Art. 5–7 DMA als formales Verletzungsverfahren sind an dieser Stelle zwei weitere Besonderheiten herauszustellen. Zum einen sieht der DMA das neue Instrument der – nicht weiter definierten – Marktuntersuchung an verschie-

---

[66] Art. 6 Abs. 4, 7, 12; Art. 7 DMA.
[67] Art. 5 Abs. 3, 4, 5, 7, 8; Art. 6 Abs. 3, 5, 6 DMA.
[68] Art. 5 Abs. 1, 6; Art. 6 Abs. 13 DMA.
[69] KOM, Commission Staff Working Document. Impact Assessment Report, Brussels, 15.12. 2020, SWD(2020) 363 final, 53 ff.
[70] BKartA, Beschl. v. 6.2.2019 – B6-22/16 (Facebook).
[71] KOM, Entsch. v. 27.6.2017 – Fall AT.39740 – (Google Search [Shopping]).
[72] *Podszun*, in: Podszun, HK-DMA, 2023, Einl. Rn. 21.
[73] Ebd. Rn. 42.

denen Stellen vor. Zum anderen nennt der DMA ausdrücklich die Verhängung von strukturellen Abhilfemaßnahmen unter der konkreten Voraussetzung der systematischen Nichteinhaltung von DMA-Pflichten. Die Einleitung von Marktuntersuchungen sieht der DMA in drei Fällen vor: Die Kommission kann eine Marktuntersuchung durchführen, um ein Unternehmen als Torwächter zu benennen (Art. 17 DMA), um eine systematische Nichteinhaltung der DMA-Pflichten zu ermitteln (Art. 18 DMA) und um den DMA-Anwendungsbereich um neue zentrale Plattformdienste oder Verhaltensregeln zu ergänzen (Art. 19 DMA).

Strukturelle Abhilfemaßnahmen sind wiederum als Ergebnis einer Marktuntersuchung nach Art. 18 DMA in Folge systematischer Nichteinhaltung möglich. Für diese greift die Vermutungsregel des Art. 18 Abs. 3 DMA, wonach eine systematische Nichteinhaltung bei drei Nichteinhaltungsbeschlüssen innerhalb von acht Jahren vermutet wird. Auch wenn strukturelle Abhilfemaßnahmen wie Unternehmensentflechtungen im *ultima ratio*-Fall grundsätzlich auch Instrument des kartellrechtlichen Werkzeugkastens sind, lässt die ausdrückliche Nennung der Voraussetzungen in Art. 18 Abs. 3 DMA strukturelle Abhilfemaßnahmen im DMA-Kontext greifbarer erscheinen.

*d) Zentralisierungs- und Harmonisierungswirkung*

Anders als das Kartellrecht verfügt der DMA über eine starke Zentralisierungswirkung, die sich nicht nur in einem Durchsetzungsmonopol der Kommission zeigt (die damit ihr Kompetenzrepertoire erheblich aufgewertet hat), sondern auch in der Normierung des Konkurrenzverhältnisses zu mitgliedstaatlichen Parallelregelungen. Die Rolle der nationalen Behörden wird für die Durchsetzung des DMA lediglich auf ein unterstützendes Tätigwerden begrenzt, vgl. Art. 37 DMA. Dieser enge Rahmen schlägt sich auch in dem mit der 11. GWB-Novelle in das deutsche Wettbewerbsrecht eingeführte § 32g GWB nieder, nach dem das Bundeskartellamt zwar Untersuchungen wegen möglicher Nichteinhaltung von Art. 5–7 DMA durchführen darf, der Kommission jedoch dazu Bericht erstattet. Eine abschließende Entscheidung in Form eines Nichteinhaltungsbeschlusses obliegt allein der Kommission.

Zudem schließt der auf die Harmonierungskompetenz aus Art. 114 AEUV gestützte DMA eine parallele Anwendung von ähnlich gelagerten nationalen Vorschriften weitestgehend aus. Das Konkurrenzverhältnis zwischen dem DMA und nationalem Regulierungs- bzw. Kartellrecht ist in Art. 1 Abs. 5 und Abs. 6 DMA geregelt; es gilt als komplex. Um eine Fragmentierung des Binnenmarkts durch die Regulierung der global agierenden Plattformunternehmen durch nationale Regelungen zu verhindern, schließt Art. 1 Abs. 5 DMA weitere mitgliedstaatliche Regelungen aus, die das gleiche Ziel wie der DMA haben, bestreitbare und faire Märkte zu gewährleisten, und in den Anwendungsbereich des DMA fallen.[74] Als *lex specialis*

[74] *König*, in: Säcker/Bien/Meier-Beck/Montag, MünchKommWettbR I, 4. Aufl., 2023, Art. 1 DMA Rn. 26 ff.

ermöglicht Art. 1 Abs. 6 DMA die komplementäre Anwendung nationaler Kartellrechtsvorschriften neben dem DMA unter bestimmten Bedingungen. Insbesondere nationales Kartellrecht, das andere Formen einseitiger Verhaltensweisen als Art. 102 AEUV verbietet, findet nur insoweit Anwendung, als dass nationale Wettbewerbsvorschriften nicht auf Torwächter angewendet werden oder weitere Verpflichtung als im DMA enthalten auferlegen, vgl. Art. 1 Abs. 6 lit. b DMA.[75] Auch wenn der deutsche Bundesgerichtshof vor kurzem die Rechtsfrage geklärt hat, dass § 19a GWB nationales Kartellrecht ist und nicht gesperrtes Regulierungsrecht nach Art. 1 Abs. 5 DMA,[76] verbleibt für nationales Wettbewerbsrecht wie § 19a GWB nur ein geringer Anwendungsbereich.

## V. Paradigmenwechsel im Wettbewerbsrecht

Nach Jahren sogenannten *Underenforcements* des Kartellrechts und einer Reihe von durchgewinkten Fusionskontrollfällen weisen neue Interventionsmodelle zur Regulierung der Marktmacht der Digitalkonzerne – ob in Form von kartellrechtlichen Reformen wie § 19a GWB oder neuen regulierungsrechtlichen Gesetzen wie dem DMA – deutlich auf einen disruptiven Paradigmenwechsel in der Wettbewerbsrechtsdurchsetzung hin. Ob dieser Paradigmenwechsel auch Impulse für Sektoren außerhalb der Digitalwirtschaft setzt, ist noch nicht abzusehen.

### *1. Abkehr vom Fokus auf Effizienz*

Anders als im Kartellrecht gewährt der DMA keine Rechtfertigungsmöglichkeiten durch Effizienzvorteile.[77] Die DMA-Pflichten gelten nur in absoluten Ausnahmefällen nicht: Erforderlich für eine Aussetzung des Pflichtenprogramms sind außergewöhnliche Umstände, auf die der Torwächter keinen Einfluss hat und die die Rentabilität seiner Geschäftstätigkeit gefährden würden (Art. 9 DMA). Eine Befreiung ist ausschließlich möglich aus Gründen der öffentlichen Gesundheit oder der öffentlichen Sicherheit (Art. 10 DMA). Während die Entscheidung der gesetzgebenden EU-Institutionen gegen eine Rechtfertigungsmöglichkeit durch Effizienzvorteile wie im Kartellrecht zulasten von Flexibilität und passgenauerer Abbildung der konkreten Umstände des Einzelfalls geht, ermöglicht der Verzicht auf ein individuelles Abwägen von Vor- und Nachteilen, einige der oben genannten Schwächen des Kartellrechts auszugleichen. Das Ausklammern der Auswertung ausführlicher Effizienzvorträge durch die betroffenen Unternehmen trägt maßgeblich zu einer Verfahrens-

---

[75] *Brauneck*, Der Digital Markets Act (DMA) – das neue, bessere digitale EU-Wettbewerbsrecht? RDi 2023, 27; *Käseberg/Gappa*, in: Podszun, HK-DMA, 2023, Art. 1 DMA Rn. 21 ff.

[76] BGH, Beschl. v. 23.4.2024 – KVB 56/22 (Amazon).

[77] *Bueren/Weck*, in: Säcker/Bien/Meier-Beck/Montag, MünchKommWettbR I, 4. Aufl., 2023, Art. 5 DMA Rn. 266 ff.

verschlankung bei.[78] Gleichzeitig etabliert der Pflichtenkatalog des DMA so auch eine einheitliche Anwendung über verschiedene Plattformdienste hinweg – damit werden substantielle Prinzipien für die digitale Wirtschaft geprägt.

Das entstehende Risiko von *Overenforcement* und *Type-I-Errors* hat der deutsche Gesetzgeber hingegen mit in den Tatbestand des § 19a GWB aufgenommen. Dieser eröffnet in § 19a Abs. 2 S. 2 GWB die Möglichkeit der sachlichen Rechtfertigung. Auch diese Rechtfertigungsmöglichkeit ist jedoch einschränkend im Lichte der gesetzgeberischen Zielsetzung des § 19a GWB zu verstehen. Die Verbotstatbestände in § 19a GWB sollen verhindern, dass Plattformunternehmen weiter durch nicht auf Leistungswettbewerb beruhenden Praktiken auf Märkten expandieren und ihre Marktstellung ausbauen, auf denen eine solche Entwicklung durch Netzwerkeffekte begünstigt wird.[79] Einschränkend darf demnach auch eine sachliche Rechtfertigung nicht aufgrund von kurzfristigen Effizienzvorteilen erfolgen, sondern muss vielmehr in der Interessensabwägung hinter dem gesetzgeberischen Ziel, Märkte für Wettbewerbschancen zu öffnen und wirtschaftliche Macht langfristig zu begrenzen, zurücktreten.[80] Insgesamt rückt die Ordnung der Märkte vom Effizienzparadigma und entsprechenden ökonomischen Theorien ab.

### *2. Abkehr vom Marktbezug*

Während die Marktabgrenzung für alle Durchsetzungssäulen des Kartellrechts als Fundament der wettbewerblichen Beurteilung dient, kommt ihr bei der Regulierung von digitalen Plattformmärkten eine untergeordnete Rolle zu. Die Schwächen der klassischen Marktabgrenzung, die tatsächlichen wirtschaftlichen Verhältnisse auf den Plattformmärkten abzubilden, haben zu einer Abkehr von der Marktorientierung geführt. Der Begriff der Marktabgrenzung findet im DMA keinerlei Erwähnung. Der DMA knüpft seinen Anwendungsbereich vielmehr an die Torwächterstellung als zentralen Mechanismus an, der maßgeblich auf quantitativen Schwellenwerten wie Marktkapitalisierung und Nutzerzahlen beruht. Diese quantitative Bestimmung entspricht dem formalisierten Regulierungsansatz des DMA und verzichtet, anders als die Marktabgrenzung im Kartellrecht, auf eine ökonomische Analyse von Marktverhältnissen.[81] Auch § 19a GWB räumt der Marktabgrenzung eine eher nachrangige Stellung ein. Nach § 19a Abs. 1 S. 1 Nr. 1 GWB kann das Bundeskartellamt zwar die marktbeherrschende Stellung des betroffenen Unternehmens auf einem oder mehreren Märkten berücksichtigen, jedoch nur als eines von insgesamt fünf, nicht zwingenden Kriterien. Marktbeherrschung auf einem bestimmten Markt ist folglich nicht

---

[78] Vgl. zum Problem langer Verfahrensdauern *Laitenberger/Kröger*, ZEuP 2023, 621 (624); *Heinemann*, Concurrences 2021, Iss. 4, 2 (2).

[79] *Wolf*, in: Säcker/Bien/Meier-Beck/Montag, MünchKommWettbR I, 4. Aufl., 2023, § 19a GWB Rn. 84.

[80] BegrRegE 10. GWB-Novelle, BT-Drs. 19/23492, 77.

[81] *Käseberg/Gappa*, in: Podszun, HK-DMA, 2023, Art. 3 DMA Rn. 2.

mehr konstitutives Element, sondern verfügt lediglich noch über (starke) Indizwirkung im Rahmen des § 19a GWB.[82]

Die Abkehr von der Marktorientierung hin zu neuen Anknüpfungskriterien wie der Torwächterstellung oder der überragenden marktübergreifenden Bedeutung für den Wettbewerb ist Ausdruck des Beschleunigungsgedankens und dient maßgeblich dem Zweck, durch den Verzicht auf langwierige Feststellungen zur Marktbeherrschung und Marktabgrenzung Verfahren zu verkürzen.[83] Zudem stoßen Kriterien der klassischen Marktabgrenzungspraxis durch erhebliche Komplexitäten und Besonderheiten der Plattformökonomie an ihre Grenzen. Die erforderliche Rechtsklarheit neuer Anknüpfungskonzepte erfordert schnelle gerichtliche Klärung offener Rechtsfragen. Auf deutscher Ebene ist dies mit der Bestätigung der überragenden marktübergreifenden Bedeutung von Amazon durch den Bundesgerichtshof als erst- und letztinstanzliches Gericht bereits erfolgt.[84] Gleiches gilt – wenn auch nicht letztinstanzlich – auf europäischer Ebene. Das Gericht der Europäischen Union hat die Torwächterbenennung des chinesischen Konzerns ByteDance bestätigt und erste gerichtliche Linien gesetzt.[85]

*3. Schutz gewerblicher Nutzer (und Wettbewerber)*

Ebenfalls in Abgrenzung zum Kartellrecht ist der Fokus auf Konsumentenwohlfahrt im Sinne der Steigerung der Konsumentenrechte kein zentrales Ziel der neuen Interventionsmodelle gegen Digitalkonzerne. Auch wenn der DMA als gesetzgeberisches Ziel die Gewährleistung bestreitbarer und fairer Märkte im digitalen Sektor zum Vorteil gewerblicher Nutzer und Nutzerinnen sowie Endnutzer und Endnutzerinnen festlegt,[86] dienen die Ziele Bestreitbarkeit und Fairness doch in erster Linie den gewerblichen Nutzern und Nutzerinnen der Torwächter. Beispielhaft kann die Stellung von Hotels gegenüber Booking genannt werden: Die Hotelbetriebe sind in Abhängigkeiten geraten, von denen sie der DMA teilweise befreien soll oder bei denen der DMA ihnen zu einer besseren Verhandlungsposition verhelfen soll. Verbraucherinnen und Verbraucher stehen nicht in gleicher Weise im Fokus. Sowohl die weit überwiegende Mehrheit der Verpflichtungen des DMA als auch der Verbotstatbestände des § 19a GWB dienen dazu, Wettbewerbsschranken zugunsten der gewerblichen Nutzer und Nutzerinnen abzubauen, etwa die Verbote von Selbstbevorzugungs- und Kopplungspraktiken oder Zugangsverpflichtungen zu Funktionen und Daten.[87] Aufgrund der wirtschaftlichen Tätigkeit der Torwächter auf unterschiedlichen, durchin-

---

[82] *Wolf*, in: Säcker/Bien/Meier-Beck/Montag, MünchKommWettbR I, 4. Aufl., 2023, § 19a GWB Rn. 23.

[83] *Käseberg/Gappa*, in: Podszun, HK-DMA, 2023, Art. 3 DMA Rn. 1; BegrRegE 10. GWB-Novelle, BT-Drs. 19/23492.

[84] BGH, Beschl. v. 23.4.2024 – KVB 56/22 (Amazon).

[85] EuG, Urt. v. 17.7.2024 – Rs. T-1077/23 (ByteDance/Kommission).

[86] Vgl. Art. 1 Abs. 1 DMA.

[87] Vgl. ErwGr. 32 DMA.

tegrierten Marktstufen innerhalb ihres Ökosystems treten Torwächter in der Regel nicht nur als Plattformbetreibende, sondern gleichzeitig auch als Anbietende auf der Plattform auf und befinden sich damit im Wettbewerb mit den eigenen gewerblichen Nutzenden. Demnach ist hinter dem Schutz der gewerblichen Nutzenden vor Praktiken der Torwächter, die geeignet sind, Bestreitbarkeit und Fairness auf Märkten zu schmälern, gleichzeitig eine Förderung von Wettbewerbern zu sehen. Dagegen räumen wenige der neu geschaffenen Verhaltenspflichten und Verbotstatbestände unmittelbare Vorteile zugunsten der Verbraucher und Verbraucherinnen ein. Art. 5 Abs. 2 DMA sowie § 19a Abs. 2 S. 1 Nr. 4 GWB bezwecken beispielsweise, Verbrauchern und Verbraucherinnen die Entscheidungshoheit über die Verwendung ihrer Daten zurückzugeben. Dass die neu geschaffenen Pflichten letztendlich auch dazu dienen sollen, Verbrauchern und Verbraucherinnen eine reichere Angebotsauswahl auf digitalen Märkten, innovativere Produkte und Dienste und ggf. auch Preissenkungen zu verschaffen, scheint insgesamt eher ein nachgelagertes, reflexhaft erreichtes Ziel zu sein.[88] Im Kartellrecht hatte sich demgegenüber eine starke Orientierung an den Vorteilen für Verbraucherinnen und Verbraucher herausgebildet.

### *4. Regeln statt Standards*

Der DMA als striktes Regelwerk bestehend aus *per se*-Pflichten und in abgeschwächter Form auch der § 19a GWB durch die konkretisierte Verbotsliste in Abs. 2 brechen in disruptiver Weise mit dem bislang vorherrschenden Ansatz im Kartellrecht.[89] Um das ultimative Ziel des Kartellrechts, den Schutz des Wettbewerbs, operabel zu machen, sind Standards (Generalklauseln) erforderlich, die den Rahmen für Feststellungen bilden, ob Ergebnisse mit der Zielsetzung des Kartellrechts übereinstimmen.[90] Während die Bestimmung, Definition und der Geltungsanspruch einzelner Standards im Kartellrecht von Diskurs geprägt sind,[91] enthält der DMA (und in Abstrichen auch § 19a GWB) klare Vorgaben, die dem Diskurs entzogen sind. Die Intention hinter dem Wandel von generalklauselartigen Bestimmungen (*standards*) zu Regeln

---

[88] *König*, in: Säcker/Bien/Meier-Beck/Montag, MünchKommWettbR I, 4. Aufl., 2023, Art. 2 DMA Rn. 114.

[89] *Kerber*, Taming tech giants with a per se rules approach? The Digital Markets Act from the „rules vs. standard" perspective, Concurrences 2021, Iss. 3, 1.

[90] OECD, The Consumer Welfare Standard – Advantages and Disadvantages Compared to Alternative Standards, OECD Competition Policy Roundtable Background Note, 2023, 9, abrufbar unter www.oecd.org/daf/competition/consumer-welfare-standard-advantages-and-disadvantages-to-alternative-standards-2023.pdf (Abrufdatum: 24.7.2024).

[91] Vgl. *Steinbaum/Stucke*, The Effective Competition Standard. A New Standard for Antitrust, University of Chicago Law Review 2020, Vol. 87 Iss. 2, 595; *Hovenkamp*, Antitrust: What Counts as Consumer Welfare? Faculty Scholarship at Penn Carey Law, 2020, abrufbar unter https://scholarship.law.upenn.edu/faculty_scholarship/2194 (Abrufdatum: 24.7.2024); *Khan*, The New Brandeis Movement: America's Antimonopoly Debate, Journal of European Competition Law & Practice 2018, Vol. 9 Iss. 3, 131; *Vaheesan*, The Profound Nonsense of Consumer Welfare Antitrust, The Antitrust Bulletin 2019, Vol. 64 Iss. 4, 479, abrufbar unter https://doi.org/10.1177/0003603X19875036 (Abrufdatum: 24.7.2024).

(*rules*) in der digitalen Plattformökonomie ist naheliegend. Klare Regeln minimieren den Ermittlungs- und Bewertungsaufwand von Behörden zur Feststellung von Verstößen und sind so geeignet, schneller Ergebnisse und Verbesserung der Marktbedingungen zu erreichen. Gleichzeitig wird die Fehleranfälligkeit durch Abbau von Flexibilität und Differenzierungsmöglichkeiten erhöht.[92] Dieser Effektivitätsvergleich von präzisen Regeln versus offenen Standards ging für die Plattformökonomie zulasten von Standards aus.[93] Insbesondere die Gefahren im Zusammenhang mit dem *Tipping* von Plattformmärkten aufgrund hoher Netzwerk- und Skaleneffekte und die Schwierigkeiten des Kartellrechts, diese Gefahren wirksam einzudämmen, scheinen ein Inkaufnehmen der Nachteile eines präzise ausformulierten Regelwerks für große Online-Plattformen zu rechtfertigen.[94]

### *5. Institutionelle Verschiebung durch Nachweispflicht effektiver Compliance*

Kartellrechtsdurchsetzung ist von behördlichen Ermittlungen und dem Nachweis von Kartellrechtsverstößen durch die Wettbewerbsbehörden geprägt. Dieser Durchsetzungsmechanismus zur Begründung von Rechtsverstößen wurde im DMA von einem neuen Mechanismus abgelöst. Nicht die Wettbewerbsbehörden, sondern die Adressaten des DMA trifft eine umfangreiche Darlegungspflicht bezüglich der Einhaltung der DMA-Pflichten. Der Torwächter muss effektive Compliance mit der Zielsetzung des DMA und den jeweiligen Verpflichtungen nachweisen (Art. 8 Abs. 1 DMA). Der DMA richtet eine Erwartung an die Torwächter, dass diese proaktiv Maßnahmen ergreifen, um sich rechtskonform zu verhalten. Sie müssen darüber hinaus die Wirksamkeit dieser Maßnahmen nachweisen. Das steht im Gegensatz zum kontradiktorischen Verfahren des Kartellrechts, in dem die Wettbewerbsbehörden eine Nachweispflicht für Rechtsverstöße trifft.[95] Diese institutionelle Verschiebung durch die Nachweispflicht effektiver Compliance durch die Torwächter ist insbesondere von drei Besonderheiten gekennzeichnet:

Die erste betrifft die umfassenden Darlegungspflichten, die vor allem in Art. 11 DMA normiert sind. Nach dieser Vorschrift werden die Torwächter zur ausführlichen und transparenten Darlegung ihrer Compliance-Maßnahmen in einem Bericht verpflichtet. Das von der Kommission veröffentlichte Template für den Compliance-Bericht legt sehr umfassende, kleinschrittige Informationspflichten für die Torwächter dar, die von der Beschreibung jeglicher (technischer) Änderungen bis hin zur Angabe von Indikatoren zur Messung der Effektivität der ergriffenen Maßnahmen

---

[92] *Kerber*, Concurrences 2021, Iss. 3, 1 (2).

[93] Für weitere Nachweise zur Bedeutung der Kosten der Rechtsanwendung für den Effektivitätsvergleich von „Rules v. Standards" siehe *Möslein*, in: Möslein (Hrsg.), Regelsetzung im Privatrecht, 2019, 1 (19).

[94] *Bueren/Weck*, in: Säcker/Bien/Meier-Beck/Montag, MünchKommWettbR I, 4. Aufl., 2023, Art. 3 DMA Rn. 74.

[95] *Seeliger*, in: Podszun, HK-DMA, 2023, Art. 11 DMA Rn. 11; *Bueren/Weck*, in: Säcker/Bien/Meier-Beck/Montag, MünchKommWettbR I, 4. Aufl., 2023, Art. 8 DMA Rn. 28 ff.

reichen.[96] Ein Verstoß gegen die Pflicht aus Art. 11 DMA ist jedoch nicht sanktionsfähig. Für eine Bewertung, ob der Gatekeeper effektive Compliance mit der Zielsetzung des DMA und der entsprechenden Verhaltenspflichten nachgewiesen hat, kann der Umstand lückenhafter Darlegungen in den Compliance-Berichten jedoch möglicherweise Berücksichtigung finden.[97]

Daneben macht der DMA auch detaillierte Vorgaben, die die interne Unternehmensgestaltung betreffen. Nach Art. 28 DMA sind Torwächter verpflichtet, in der internen Unternehmensstruktur eine Compliance-Funktion einzurichten. Die Vorschrift enthält sowohl strukturelle als auch personelle Vorgaben.[98]

Die dritte Besonderheit betrifft die Pflicht zur Effektivitätskontrolle der ergriffenen Compliance-Maßnahmen der Torwächter. Gemäß Art. 8 Abs. 1 S. 2 DMA müssen die ergriffenen Compliance-Maßnahmen dazu führen, dass die Ziele des DMA und der jeweiligen Verpflichtung wirksam erreicht werden. Die Effektivitätskontrolle ist nicht von der Nachweispflicht der Torwächter umfasst.[99] Wann die Ziele des DMA und der Verpflichtungen im Einzelnen wirksam erreicht werden, definiert der DMA nicht und eröffnet damit einen erheblichen Auslegungsspielraum für die Kommission. Nicht genügend ist aber jedenfalls die Erfüllung dessen, was nach den Buchstaben der Verordnung verlangt wird. Vielmehr muss diese Compliance auf den Märkten wirksam sein. Das ist ein geradezu revolutionärer Ansatz.

Auch der Nachweis eines Verstoßes gegen die Verbotstatbestände in § 19a GWB wird dem Bundeskartellamt erleichtert, da die Rechtsnatur der Verbotstatbestände als widerlegliche Vermutungen einzuordnen ist.[100] Insbesondere trifft das Bundeskartellamt nicht die Pflicht, einen Nachweis einer wettbewerbsbeschränkenden Wirkung im Einzelfall zu erbringen, sondern nur, das Wettbewerbsgefährdungspotenzial eines bestimmten Verhaltens in der jeweiligen Marktumgebung zu plausibilisieren.[101]

Aufgrund der institutionellen Verschiebung des Nachweises von Rechtskonformität stellt jedenfalls der DMA ein neuartiges wirtschaftsrechtliches Ordnungsinstrument dar. Die Verordnungsgeber haben gezielt an den etablierten Nachweisanforderungen geschraubt. Ob die entsprechenden Anforderungen im DMA – und in abgeschwächter Form auch die Nachweiserleichterung des § 19a GWB – tatsächlich geeignet sind, durch diese Verschiebung Ermittlungsressourcen der Wettbewerbsbe-

---

[96] KOM, Article 11 DMA – Compliance Report Template Form, abrufbar unter https://digital-markets-act.ec.europa.eu/legislation_en#templates (Abrufdatum: 24.7.2024).

[97] *Seeliger*, in: Podszun, HK-DMA, 2023, Art. 11 DMA Rn. 12 ff.

[98] *Lahme/Ruster*, in: Podszun, HK-DMA, 2023, Art. 28 DMA Rn. 7 ff.; *Bechthold/Bosch/Brinker*, EU-Kartellrecht, 4. Aufl., 2023, Art. 28 DMA Rn. 27.

[99] *Bueren/Weck*, in: Säcker/Bien/Meier-Beck/Montag, MünchKommWettbR I, 4. Aufl., 2023, Art. 8 DMA Rn. 28.

[100] BT-Drs. 19/25868, 114; BegrRegE, BT-Drs. 19/23492, 78; kritisch *Schweitzer*, in: Immenga/Mestmäcker, Wettbewerbsrecht II, 7. Aufl., 2024, § 19a GWB Rn. 132.

[101] *Schweitzer*, in: Immenga/Mestmäcker, Wettbewerbsrecht II, 7. Aufl., 2024, § 19a GWB Rn. 134.

hörden zu schonen und schnellere Veränderungen der Marktstrukturen auf digitalen Plattformmärkten zu erzielen, bleibt abzuwarten. Widerwillige Erfüllung der Darlegungspflichten aus Art. 11 DMA betreffend den Compliance-Bericht und die Einleitung von bereits sechs Nicht-Einhaltungsverfahren innerhalb der ersten vier Monate, nachdem die bereits benannten Torwächter die DMA-Pflichten einzuhalten hatten, zeigt, dass die selbst durchsetzende Wirkung des DMA durchaus Anfälligkeiten für Startschwierigkeiten aufweist. Darüber hinaus ist derzeit offen, welche Maßstäbe die Gerichte anlegen.

## VI. Ergebnis und Ausblick

Die Reform des Kartellrechts und die Einführung neuer Interventionsmodelle, um den Anforderungen der Digitalisierung und Vormachtstellung der *Big Tech*-Plattformen gerecht zu werden, hat einen Paradigmenwechsel in der wirtschaftsrechtlichen Rechtsdurchsetzung eingeläutet. Die Herausforderungen der Plattformökonomie, allen voran Netzwerkeffekte, Mehrseitigkeit von Diensten, Datenvorteile und komplexe Ökosystemstrukturen, haben ein wirtschaftspolitisches Umdenken erforderlich gemacht. Das Kartellrecht war in seinem starken Vertrauen auf bestimmte ökonomische Konzepte und hohe Nachweisanforderungen in eine Sackgasse geraten. Zumindest zur Regulierung von digitalen Plattformmärkten scheinen klassische Konzepte zur Marktabgrenzung und ökonomische Analysen zu möglichen Effizienzvorteilen abgelöst. Die großen Plattformen stehen nun in einer noch viel stärkeren Verantwortung. Das ist mit Blick auf ihre Stellung als Infrastrukturanbieter des Internets und Regelsetzer für die Digitalwirtschaft durchaus nachvollziehbar.

Auf eine dezentrale Verteilung der Rechtsdurchsetzung zwischen Europäischer Kommission und mitgliedstaatlichen Behörden wurde durch den DMA verzichtet. Der Beweis der wirksamen Eignung der neuen Interventionsmodelle steht noch aus und wird insbesondere davon abhängen, ob die Gerichte mitziehen. Die ersten gerichtlichen Entscheidungen deuten in diese Richtung.[102] Signalwirkung über die europäischen Grenzen hinaus strahlen die Reformvorreiter, der DMA und § 19a GWB, jedenfalls aus.

[102] BGH, Beschl. v. 23.4.2024 – KVB 56/22 (Amazon); EuG, Urt. v. 17.7.2024 – Rs. T-1077/23 (ByteDance/Kommission).

# Digital Vulnerability as the New Legal Category to Regulate the Human-Machine Interaction*

*Amalia Diurni*



## I. The Characteristics of the Digital Revolution and the Efforts to Achieve its Governance

The starting point for any modern legal system is the concept of legal subject as an autonomous and rational adult. Actually, following Fineman's doctrine,[1] this concept needs to be replaced by that of the embodied individual who experiences vulnerability in all stages of life and in all sorts of settings. There are not just particular vulnerable groups, for the human condition itself is one of universal and constant human vulnerability. The critique of non-discrimination law with its classical liberal and

* The research for this article was funded by the Italian Ministry of Universities and Research (MUR) under the PRIN 2020 project 'Digital Vulnerability in European Private Law' and by the Istituto Italiano di Studi Germanici under the research project 'Instabilità del diritto e vulnerabilità digitale'.

[1] *Fineman*, The Vulnerable Subject: Anchoring Equality in the Human Condition, Yale Journal of Law & Feminism 2008, Vol. 20 Iss. 1, 1 (1–23).

formal insistence on the same treatment for similarly situated individuals[2] was valuable in showing the path towards a more substantive vision of equality and awareness about human condition and to exhort lawmakers to shift from a static to a dynamic approach to the human condition. The digital revolution, rapid in time and global in scope, characterised by a variety of technologies and a multidimensional and multi-layered nature, can be governed only by a forward-looking set of dynamic tools and the concept of digital vulnerability as a macro-category could be of help. Before introducing arguments in favour of the use of the concept of vulnerability in the governance of the digital revolution, an overview of the peculiarity of this digital revolution could be useful.

The digital revolution is a revolution based on invention. It is not the first time that mankind invents a new product, tool, process or concept that implies a paradigm shift. Mankind firstly needs time in order to understand the implications of the new invention in terms of advantages and risks. Secondly, it needs time in order to find the right legal instruments for addressing and preventing risks and repairing the harms caused by the new invention. A paradigm shift implies deep modifications on the economic and societal structures, and it is usually multidimensional. Exploring the consequences of a new invention that shapes the world is as complex as it is *multidimensional.* In regard to AI and digital technologies, the impacts involve social, economic, political and cultural dimensions. The digital revolution is such a multi-layered revolution that it impacts at individual and collective levels, at national, regional and international levels.

Furthermore, the digital revolution is based on a *variety* of technologies. This means that we can try to find different solutions depending on each class of products or tools, or we can – in doing this – also try to approach the issues created by this revolution to a much higher level than the practical one. The peculiarity of the digital revolution is that it is such a multi-layered and multidimensional revolution that it is difficult to find inventions in the history of mankind similar in impact, nature and characteristics. This digital revolution is of technical nature, and yet, due to the characteristics of this technology, its impacts are at a much higher level than a simple product or tool invention. Consequently, at the beginning of its diffusion it urged solutions case by case, sector by sector for operational reasons. Therefore, US courts' response to the initial anarchistic approach[3] has focused primarily on the need to protect freedom of expression, whilst the ECJ's case law has given priority to data protection. The European legislator has indeed enacted various laws stressing the legal focus on legal requirements more than on rights.[4] The result was a vertical and surgical approach, accompanied by a holistic one made of ethics codes and guide-

[2] *Fineman*, Vulnerability and Social Justice, Valparaiso University Law Review 2019, Vol. 53 Iss. 2, 341 (341–369).

[3] *Johnson*/*Post*, Law and Borders. The Rise of Law in Cyberspace, Stanford Law Review 1996, Vol. 48, Iss. 5, 1367 (1367–1402).

[4] *Hörnle*, Internet Jurisdiction Law and Practice, 2021, 436 et seqq., in particular 451.

lines, too vague and soft to be of much help. When the lack of a general and horizontal view became evident, the European approach was addressed from a vertical-sectoral to a procedure-based one as resulted by the Digital Services Package up to the apex of the Artificial Intelligence Act (AI Act).[5] The latter still considers AI systems as mere products with a regulation structured around different levels of risk. While resulting in a first and important intellectual and political effort to give a common frame of reference in the matter, the AI Act is still lacking on a single principle to serve as a general, robust and grounded criterion for the interpretation, application, adaptation and development of the present first-generation digital law and to inform any conduct related to it. The reference to human rights in Art. 27 AI Act and to an unspecified Fundamental Rights Impact Assessment (FRIA) is generic and risks turning into yet another formality that is only minimally effective in protecting individuals and society, as the GDPR's consent for data protection purposes has turned out to be.[6]

Incidentally, the concept of human rights is an invention per se. Differently from the human rights revolution, since the beginning the digital revolution spread globally. No matter where digital technologies were or are being invented, their diffusion is *worldwide*. This implies a new challenge because different contexts correspond to different impacts of digital technologies. Furthermore, although the cause is one and the same, characteristics and features of the involved countries vary as well as their effects in terms of societal reactions and public interventions. With respect to the legal instruments used to govern this revolution, even if it is global, the policies differ from country to country and from region to region in consideration of the governments' political purposes and the values to be protected. The regulatory approach is differing not just between Western and Eastern legal traditions or Global North and Global South, but among countries belonging to the same legal family.[7]

Another peculiarity of this revolution is the *rapidity* by which the first invention and all those that follow from that first are spreading within societies, changing the world deeply and in a pervasive way. The digital technologies are at the same time the cause of the digital revolution and the means for its rapid diffusion. The rapidity in the diffusion together with the fact that digital technologies are products in time of mass industrialization, are the reasons of their pervasiveness. Therefore, the first approach to the digital revolution was the use of the already in force consumer protection law, intended to address the risks coming from the new products. In particu-

---

[5] *Pollicino*, The quadrangular shape of the geometry of digital power(s) and the move towards a procedural digital constitutionalism, European Law Journal 2023, Vol. 29 Iss. 1–2, 10 (10–30).

[6] *Mantelero*, The Fundamental Rights Impact Assessment (FRIA) in the AI Act: roots, legal obligations and key elements for a model template, Computer Law & Security Review 2024, Vol. 54 article no. 106020, 1, available at http://dx.doi.org/10.2139/ssrn.4782126 (last accessed on: 31 August 2024).

[7] *Pollicino*, Judicial Protection of Fundamental Rights on the Internet. A Road Towards Digital Constitutionalism? 2021, 110 et seqq.

lar, with respect to digital products, the definition of vulnerable consumers,[8] which was launched by a study financed by the European Commission and published in 2016, is very promising.[9] The study has demonstrated that the consumer's vulnerability depends on many factors but is the result of socio-demographic and behavioural characteristics, personal situation, or market environment. In this respect, digital technologies impact pre-existing forms of vulnerability and create new ones,[10] so that consumer law is under evaluation by legal experts to understand whether it is adequate to face the new challenges coming from the digital revolution and, in the negative case, how it can be modified to be efficient in preventing new vulnerabilities or addressing the old ones exacerbated by the diffusion and use of digital technologies.[11]

The rapid and continuous development of new technologies in the field quickly renders regulations obsolete. As the result of legal studies and political compromises, regulations take time to be drafted, approved, enacted and finally implemented. It seems that there is a discrepancy between the pace of technological innovation and the ability of lawmakers to maintain effective control over its effects on individuals and communities. Despite the already mentioned regulatory efforts, the main issue remains the control of the digital revolution, fostering advantages and reducing risks. In this regard, the very key words of digital law policies are control, promotion and protection. Law is the instrument that can achieve these goals, stressing the one goal that is more suitable for the internal legal order and in compliance with the fundamentals of its identity. While different goals cause differences in regulation, a single, simple principle with a universal vocation is becoming essential for guiding the political debate and drafting common rules.

The regulation power is in the hand of lawmakers, but the legal process is more complex than it appears. *Sacco*[12] helped to understand and theorise the agents that form the law, despite the formal recognition as sources of law at the public level. In his theory, the legal formants of the law are legislators, judges and academics, who contribute, each with their own instruments and with the authority formally or operationally granted to them, to the creation of the law. Sometimes they work together, but more often they are competing with each other. To these three, perhaps there is a

---

[8] *Basu/A. Kumar/S. Kumar*, Twenty-five years of consumer vulnerability research: Critical insights and future directions, Journal of Consumer Affairs 2023, Vol. 57 Iss. 1, 673 (673–695).

[9] *European Commission, Consumers, Health, Agriculture and Food Executive Agency*, Consumer vulnerability across key markets in the European Union: executive summary, Publications Office, 2016, available at https://data.europa.eu/doi/10.2818/165625 (last accessed on: 31 August 2024).

[10] *Malgieri*, Vulnerability and Data Protection Law, 2023, 47 et seqq.

[11] Crea/De Franceschi (eds.), The New Shapes of Digital Vulnerability in European Private Law, 2024, in press.

[12] *Sacco*, Legal Formants: A Dynamic Approach to Comparative Law (Installment I of II), The American Journal of Comparative Law 1991, Vol. 39 Iss. 1, 1 (1–34); *Sacco*, Legal Formants: A Dynamic Approach to Comparative Law (Installment II of II), The American Journal of Comparative Law 1991, Vol. 39 Iss. 2, 343 (343–401).

new legal formant that is increasing its power: the practical formant. Experts and operators, corporations and private institutions in different sectors with international vocation and strategic economic value are creating digital law in two ways: by means of the contractual autonomy and on a customarily basis by sharing the same solutions and contributing to the creation of an autonomous and yet not binding body of law[13] as the new *lex mercatoria* in transnational commercial law.[14] In the digital law, the very large platforms (VLP) are not just setting the rules, but also controlling disputes through internal complaint mechanisms.[15] Their power as legal formants is demonstrated by the fact that they have forced the European institutions to follow the trend of the Online Dispute Resolution (ODR)[16] and to provide redress mechanisms (i. e. Art. 21 DSA).[17]

All these four agents are working on adapting the already existing legal framework to the new context. Nonetheless, while the challenges are similar, national and regional policies differ from one another. Considering the three most important markets in the world, namely the US, the EU and China, one might note that the purposes behind the governmental intervention on the sector are very different, while the fears arising from the rapidity and the pervasiveness of the digital revolution as well as its intrinsic outcomes are the same. The regulations of the digital economy are driven by political values: when they differ, the policies differ too.

## II. The Issues Related to the Human-Machine Interaction (HMI)

The challenges are multiple and various. The very one I want to focus on is related to the deep interaction between humans and machines in digital healthcare. The first consumer-facing browser-based LLM and Generative AI system have been launched in November 2022 by OpenAI[18] and from that moment on such systems have evolved

---

[13] *Kadour/Zoboli*, Increasing standardization for smart(er) contracts, Uniform Law Review 2021, Vol. 26 Iss. 3, 583 (583–598); *Eidenmüller/Wagner*, Law by Algorithm, 2021, 157 et seqq., 223 et seqq.; *Mattei*, The Legal Metaverse and Comparative Taxonomy: A Reappraisal, The American Journal of Comparative Law 2023, Vol. 71 Iss. 4, 900 (900–929).

[14] *Berger*, The Creeping Codification of the New Lex Mercatoria, 2010, passim; *Toth*, The Lex Mercatoria in Theory and Practice, 2014, passim.

[15] *Wagner/Eidenmüller*, Digital Dispute Resolution, SSRN 2021, 1 (1–44), available at https://ssrn.com/abstract=3871612 or http://dx.doi.org/10.2139/ssrn.3871612 (last accessed on: 31 August 2024).

[16] *Pálfi*, Internal dispute resolution systems: Do high promises come with higher expectations? Hungarian Journal of Legal Studies 2024, Vol. 64 Iss. 3, 391 (391–412).

[17] *Vilalta*, ODR for E-Commerce, in: Wahab/Katsh/Rainey (eds.), Online Dispute Resolution: Theory and Practice. A Treatise on Technology and Dispute Resolution, 1st ed., 2012, 113 (124 et seqq.); *Poblet/Ross*, ODR in Europe, in: Wahab/Katsh/Rainey (eds.), Online Dispute Resolution: Theory and Practice. A Treatise on Technology and Dispute Resolution, 1st ed., 2012, 453 (465 et seqq.).

[18] *OpenAI*, Introducing ChatGPT, November 2022. Available at https://openai.com/index/chatgpt/ (last accessed on: 31 August 2024).

continuously, opening new ways to their application. Of course, the long history of human fundamental rights affirmation briefly mentioned above, provides the operational and legal attention deserved to avoid the risks and take precautions. However, this will only be viable with the public awareness necessary for human rights' full implementation and the detection of the risks related to new technologies. Furthermore, what is needed is the capability to develop a forward-looking set of dynamic tools and affirmative actions to prevent individual harms and societal distortions.[19]

### *1. The HMI's First Step: The Unpredictable Consequences of Algorithmic Profiling*

Unfortunately, despite the development of regulations to address the challenges of the digital revolution in the US and the EU as described above, the experience of the two decades since the large-scale advent of social media and algorithmic profiling has demonstrated that it is hard work to predict the impact of new technologies on individuals and society in advance and to prevent the harms resulting thereof. Worth noting is that artificial intelligence applications in social media have represented the first step of HMI so far.[20] At this first stage, the technologies invented were used as mere tools. In this respect, algorithmic profiling is a highlighting example. While it has been used by businesses and organisations for legitimate purposes (targeted advertising, product development, risk assessment, fraud detection, personalised recommendations etc.),[21] it has raised privacy concerns about the collection and analysis of large amounts of personal data, discrimination and biases with negative impact on individuals and groups, and lack of transparency about how the algorithms themselves infer the generation of outputs from the inputs they receive or extract through scraping.[22] Actually, despite the international recognition of the relevance of the European Regulation on Data Protection, the legal toolkit provided by it seems in some cases inadequate to address the issues coming from new technologies. While the user consent requested from the General Data Protection Regulation (GDPR) shall be freely given, specific, informed and unambiguous (Art. 4 para. 11 GDPR), demonstrable and withdrawable (Art. 7 para. 1 and 3 GDPR), research on users' online behaviour has revealed the privacy paradox, namely the discrepancy existing between user attitude and their actual behaviour.[23] Due to the Dual Process Model of Cogni-

---

[19] *Bossuyt*, International Human Rights Protection: Balanced, Critical, Realistic, 2016, 43 et seqq.

[20] *Schleidgen/Friedrich/Gerlek/Assadi/Seifert*, The concept of 'interaction' in debates on human-machine interaction, Humanities and Social Sciences Communications 2023, Vol. 10, 551;*Esposito*, Artificial Communication. How Algorithms produce Social Intelligence, 2022, 1–18.

[21] *Tzoulia*, Targeted Advertising in the Digital Era: Modern Challenges to Consumer Privacy and Economic Freedom: The Responses of the EU Legal Order, in: Synodinou/Jougleux/Markou/Prastitou-Merdi (eds.), EU Internet Law in the Digital Single Market, 2021, 447.

[22] *Pasquale*, The Black Box Society: The Secret Algorithms That Control Money and Information, 2015, passim.

[23] *Barth/De Jong*, The Privacy Paradox – Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review, Telematics and Infor-

tion,[24] threats to privacy and actionable protective measures are often overlooked in exchange for quick access to the service being offered and/or a more engaging and satisfying online experience. In the case of digital healthcare, these distortions may be even more disruptive because of the particular vulnerability of the patient.[25]

Algorithmic profiling was the first step to a sort of interaction with AI. It was supposed to help improve efficiency, accuracy and personalization. Despite the excellent results achieved in this direction, the distortions produced are still far from being addressed by the current regulation. The creation of filter bubbles and echo chambers by the recommendation algorithms limits the users' exposure to diverse perspectives, reinforces pre-existing biases, hinders the opportunity for informed discussion and compromise, and contributes to the current polarisation of political debate.[26] By personalising content, algorithms exploit and amplify confirmation biases unintentionally and unpredictably. Users are exposed to emotional manipulation and algorithmic management,[27] misinformation and disinformation.[28] While giving the users the illusion of a personalization of the interaction, algorithms have a homogenising effect on people, being designed to identify patterns in data and to reduce variables as far as possible.

Richard Thaler and Cass Sunstein explained in their seminal book about 'Nudge: Improving Decisions About Health, Wealth and Happiness'[29] how policymakers can prod behavioural changes, predictably altering people's behaviour without forbidding any opinions or significantly changing their economic incentives. As happens in the choice architecture for data privacy, individuals are free to opt-out, but the nudge is designed to influence them to act in a preferred way. This is even more powerful when it is an algorithm that is nudging.[30]

---

matics 2017, Vol. 34 Iss. 7, 1039 (1039–1058); *Waldman*, Cognitive biases, dark patterns, and the 'privacy paradox', Current Opinion in Psychology 2020, Vol. 31, 105 (105–109).

[24] *Kahneman*, A perspective on judgement and choice: mapping bounded rationality, American Psychologist 2003, Vol. 58 Iss. 9, 697 (697–720).

[25] *Hurst*, Vulnerability in research and health care; describing the elephant in the room? Bioethics 2008, Vol. 22 Iss. 4, 191 (191–202).

[26] *Tucker/Guess/Barbera/Vaccari/Siegel/Sanovich/Stukal/Nyhan*, Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature, SSRN, 2018, 1 (1–95).

[27] *Lee/Kusbit/Metsky/Dabbish*, Working with Machines: The Impact of Algorithmic and Data-Driven Management on Human Workers, in: Association for Computing Machinery (ed.), Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15), 2015, 1603 (1603–1612).

[28] *Guess/Lyons*, Misinformation, Disinformation, and Online Propaganda, in: Persily/Tucker (eds.), Social Media and Democracy, 2020, 10 (10–33).

[29] *Thaler/Sunstein*, Nudge: Improving Decisions About Health, Wealth and Happiness, 2009, passim.

[30] *Möhlmann*, Algorithmic Nudges Don't Have to Be Unethical, Harvard Business Review, 2021, available at https://hbr.org/2021/04/algorithmic-nudges-dont-have-to-be-unethical (last accessed on: 31 August 2024).

*2. The HMI's Second Step: The Conversational Agents (CAs)*

The new frontier of digital revolution is the application of CAs, including embodied CAs, chatbots, and socially assistive robots (SARs) for the interaction with users.[31] Among many others, the major concern is in my opinion the polished ability of these robots to mimic human conversation. Indeed, in their exchanges, chatbots are able to express empathy and impressive erudition, mixed with arrogant assertiveness and variability of tone (friendly, excited, stable, serious) and style (professional, informative, educational, storytelling, benefit-focused or solution-oriented). The constant performance improvement occurs through complex attention mechanisms that enable the bots to focus on specific parts of the input text to generate more relevant and accurate outputs with respect to context, recipients' personalities and their wishes. Furthermore, the ability to store input information from the same user in memory modules makes questioning and answering exchanges more coherent and similar to those between humans. But whilst chatbot answers may seem 'sensible', they actually make 'no sense' to the machines whatsoever. And this is where the most insidious threat lies, because chatbots are modelled to imitate human conversation, thus making it hard to recognise responses as 'artificial'. It is for this very reason that the chatbots must, by default, warn users of their nature. In the digital healthcare, for example, while highlighting the potential contributions of this new technology to clinical practice in the field,[32] the particular interaction between humans and machines developed through CAs outside the healthcare sector and the risks observed[33] raise more concerns when people with recognised vulnerabilities as patients, minors, elders or disabled people are involved.

*a) The Threats from an Epistemological Perspective*

Whilst the ability of chatbots to assimilate syntactic rules endows their responses with impressive linguistic consistency, the modest writing ability of the average user puts the latter in a position of inferiority *vis-à-vis* the machine. This condition of perceived or actual inferiority constitutes a prerequisite for vulnerability. Beyond any form of 'amusement',[34] 'intellectual' challenge[35] or professional use of chatbots (by experts capable of appraising the reliability of responses), most users who ques-

---

[31] *Kiuchi/Otsu/Hayashi*, Psychological insights into the research and practice of embodied conversational agents, chatbots and social assistive robots: a systematic meta-review, Behaviour & Information Technology 2023, ahead-of-print, 1 (1–41).

[32] *Viduani/Cosenza/Araújo/Kieling*, Chatbots in the Field of Mental Health: Challenges and Opportunities, in: Passos/Rabelo-da-Ponte/Kapczinski (eds.), Digital Mental Health 2023, 133.

[33] *Pasquale*, New Laws of Robotics. Defending Human Expertise in the Age of AI, 2020, 33 et seqq.; *de Graaf/Peter*, Human Social Relationships with Robots, in: Guzman/McEwen/Jones (eds.), The SAGE Handbook of Human–Machine Communication, 2023, 435 (435–442).

[34] *Thorp*, ChatGPT is fun, but not an author, Science 2023, Vol. 379 Iss. 6630, 313.

[35] *Floridi/Chiriatti*, GPT-3: Its Nature, Scope, Limits, and Consequences, Minds and Machines 2020, Vol. 30, 681 (681–694).

tion a chatbot are technically inexperienced and not competent in the subject matter. For such users chatbots are neither entertainment nor work, but tools to understand reality. So, in addition to the danger of spreading misinformation that has been detected, the inferior subject's proneness to rely on those who are perceived to be more experienced, capable and educated alters the normal course of the interaction. Whilst this is common in interactions between humans – so much so that experts take responsibility for what they say – in interactions with CAs users are warned of the nature and limits of the bot and, in accordance with the terms of use, are held solely responsible for their prompts, the CAs responses that ensue, and the use that is made of such responses. The manner in which warnings are given and terms of use are accepted does not prevent users from consciously or unconsciously perceiving epistemological value in the chatbot's responses. The syntactic accuracy of the bot's answers and the adjustment of tone and style to match those of the questions are not, of course, the result of any consciousness nor sensitivity of the machine, but interlocutors are, nonetheless, led to perceive them as being endowed with both. Scientists' warnings[36] about NLG's lack of empathy, semantic cognition or attribution of meaning have been to no avail. The mirror with which AI reflects their image back onto humans is both deceiving and beguiling.[37] Thus, the danger is to witness a human preference, at the micro level, for perpetually available, educated, accommodating and benevolent artificial conversation[38] and for the 'truth' generated by them instead of expert's indications, like medical, legal or technical instructions. At the macro level, the threat lies in the deliberate or accidental manipulation of reality and human knowledge as generated by 'meaningless' AI narratives.[39]

Furthermore, there are impacts also on the dynamics of social interaction under a sociological profile.

*b) The Threats from a Sociological Perspective*

In its digital interactions, human vulnerability undoubtedly emerges as a characteristic of the individual. Since individuals are 'interdependent people in the singular',

---

[36] *McQuillan*, Data Science as Machinic Neoplatonism, Philosophy and Technology 2018, Vol. 31 Iss. 2, 253 (253–272); *Bender/Gebru/McMillan-Major/Shmitchell*, On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? in: Association for Computing Machinery (ed.), FAccT '21: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency, 2021, 610 (623); *Arkoudas*, ChatGPT is no stochastic parrot. But it also claims that 1 is greater than 1, Philosophy & Technology 2023, Vol. 36 article no. 54, 1 (1–29).

[37] *Prem*, Our Digital Mirror, in: Werthner/Prem/Lee/Ghezzi (eds.), Perspectives on Digital Humanism, 2022, 89 (89–94).

[38] *De Paoli et al.*, Authenticity by Design: Reflections on Researching, Designing and Teaching Socialbots, in: Gehl/Bakardjieva (eds.), Socialbots and Their Friends. Digital Media and the Automation of sociality, 2016, 164 (164–187).

[39] *Floridi*, The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities, 2023, passim; *Bishop*, Artificial Intelligence Is Stupid and Causal Reasoning Will Not Fix It, Frontiers in Psychology 2021, Vol. 11 article no. 513474, 1.

vulnerability also pertains to the whole of society, as it is composed of 'interdependent people in the plural'.[40] The ability of CAs to imitate human communication directly threatens the individuals with whom they interact and indirectly threatens the entire society. The communication is not authentic but appears so. The answers to questions, which seem original and full of new content, are, in fact, merely syntactically ordered and stylistically elegant reformulations of existing content. The process of retrieving archived content takes place automatically according to the law of the most probable.[41] Chatbots do nothing more than perpetuate the most quantitatively prevalent data (and not the most qualitatively or ethically superior data) through an iteration of logical models, with no critical capability or semantic awareness whatsoever.[42] If communication is a form of symbolic construction of reality, then the massive proliferation of communicative agents cannot but affect the construction mechanism of the representation that individuals have of themselves, of the society they belong to, and of the environment they live in.[43] It is impossible to predict how the entry of AI as a new individual and social interlocutor will change psychological and sociological dynamics and whether it will be disruptive or beneficial. However, given this uncertainty, it would be advisable not to take risks, and avoid exposing users to such risks without any caution. While the experience made with regard to the first-stage of HMI suggests to act carefully, the message didn't pass to the big tech companies, considering the launch of new technologies as OpenAI's ChatGPT without any prior public check and authorization.

## III. The Digital Vulnerability as Leading Tool to Govern the Digital Revolution

The free ChatGPT application launched in November 2022 was a sort of mass experiment. The analysis of how the algorithm works revealed several critical concerns and initiated the legal debate on CAs at two levels: a specific one, with reference to chatbots, and a general one, with reference to any future AI product that might be launched without prior public scrutiny.

---

[40] *Elias*, The Civilizing Process. The Development of Manners, 1978, passim.

[41] *Bertolaso/Marcos*, Umanesimo tecnologico. Una riflessione filosofica sull'intelligenza artificiale, 2023, 56 et seqq.

[42] *Floridi*, AI as Agency Without Intelligence: on ChatGPT, Large Language Models, and Other Generative Models, Philosophy & Technology 2023, Vol. 36 article no. 15, 1.

[43] *Hepp et al.*, ChatGPT, laMDA, and the hype around communicative AI: The automation of communication as a field of research in media and communication studies, Human-Machine Communication 2023, Vol. 6, 41 (41–63).

*1. With Regard to Chatbots*

With regard to ChatGPT, the Italian Data Protection Authority has taken *a posteriori* actions to demonstrate the uselessness of the ban instrument and the inadequacy of the GDPR to deal with threats posed by this new technology. Regarding both, the enforcement action taken by the Italian Data Protection Authority and the inadequacy of GDPR, on 13 April 2023 European Data Protection Board members decided to launch a dedicated task force to foster cooperation on the matter. In general, the fall of 2023 witnessed multiple political reactions to ChatGPT: the UK White Paper on AI,[44] the Chinese Cyberspace Administration Draft Measures for managing generative AI[45] and the EU Parliament amendments to the Commission's AI Act Proposal.[46] Concerns about the spread of chatbots and the possible threats associated with them have also emerged at an international level, triggering a number of initiatives already underway and several others that are in the pipeline: UNESCO's Guidance for generative AI in education and research; G7's 'Hiroshima Process'[47] with the International Guiding Principles[48] and the International Code of Conduct for Organizations Developing Advanced AI Systems;[49] the Bletchley Declaration.[50]

*2. On a General Level*

An analysis of government strategies on the topic of artificial intelligence reveals several different positions on the matter, some preferring mild guidelines and others

---

[44] *Department for Science, Innovation and Technology and Office for Artificial Intelligence (UK)*, A pro-innovation approach to AI regulation, Command Paper no. 815, 29 March 2023 (Updated 3 August 2023) (White Paper, 2023). Available at https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper (31 August 2024).

[45] *Cyberspace Administration of China*, Interim Measures for the Management of Generative Artificial Intelligence (AI) Services, 10 July 2023 (IMMGAIS, 2023), available at https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm (last accessed on: 31 August 2024).

[46] EU Parliament amendments to the Commission's AI Act Proposal, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM[2021]0206 – C9-0146/2021 – 2021/0106[COD]), 14 June 2023 available at https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html (last accessed on: 31 August 2024).

[47] *Group of Seven (G7)*, Statement on the Hiroshima AI Process, 30 October 2023. Available at https://www.soumu.go.jp/hiroshimaaiprocess/pdf/document01_en.pdf (last accessed on: 31 August 2024).

[48] *Group of Seven (G7)*, Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI system, 30 October 2023. Available at https://www.mofa.go.jp/files/100573471.pdf (last accessed on: 31 August 2024).

[49] *Group of Seven (G7)*, Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems, 30 October 2023. Available at https://www.mofa.go.jp/files/100573473.pdf (last accessed on: 31 August 2024).

[50] Bletchley Declaration signed by the countries attending the AI Safety Summit in UK on 1 November 2023. Available at https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration (last accessed on: 31 August 2024).

strict regulatory laws. However, recent debates and actions at national, regional and global levels all seem to converge towards the search of new regulatory forms and political strategies with variable geometry and force;[51] one that falls between intersectoral guidelines and hard laws, between sectoral codes of conduct and public authority controls, between business lobbying and democratic empowerment. The Organisation for Economic Co-operation and Development has put together a regulatory policy with an agile and innovative approach, which describes tools to address digital era challenges such as regulatory sandboxes, behavioural insights, risk-based and outcome-based regulations.[52]

There seem to be two directions along which political action is moving to try to regain control over fast-emerging technology: These are, on the one hand, to require that AI producers establish, implement, document and maintain a risk management system with third-party verification and comply with duties of transparency, explanation and provision of information to users, and, on the other hand, to introduce procedures and authorities to control new technologies before their mass distribution. The latter solution has been adopted by the AI regulatory sandboxes of the European AI Act, the UK White Paper, and President *Biden's* Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence.[53]

As for obligations of transparency, risk assessment and explainability, the problem lies in the difficulty of predicting risks. The more the AI is advanced, the less predictable its logical-mathematical processes, decisions and outputs are. To require that only inherently controllable algorithmic models (i. e. ones that are predictable *ex-ante* or re-constructible *ex-post*) are being used is unreasonable. This would result in the prohibition of self-training, deep learning, generative AI systems, for which this kind of protectionist intervention is to be excluded. The consequence of the application of advanced AI systems with conversational skill is an increasingly deep and pervasive HMI, with all the unknowns that go with the radical paradigm shift induced by the communicative agents with unprecedented features in human history.

---

[51] *C. Vanberghen/A. Vanberghen*, AI Governance as a Patchwork: The Regulatory and Geopolitical Approach of AI at International and European Level, in: Synodinou/Jougleux/Markou/Prastitou-Merdi (eds.), EU Internet Law in the Digital Single Market, 2021, 233.

[52] *Organization for Economic Co-operation and Development (OECD)*, Recommendation of the Council on Regulatory Policy and Governance, 2 November 2012. Available at https://doi.org/10.1787/9789264209022-en (last accessed on: 31 August 2024).

[53] *US President Biden*, Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 30 October 2023. Available at https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ (last accessed on: 31 August 2024).

## IV. In the Global Perspective

Waiting at first for the development of practices and guidelines in EU in order to apply the FRIA provided for in the AI Act in an effective and robust way and at a later stage by means of the Brussels effect,[54] it might be useful to analyse whether and how the policies in respect of the paradigm shift caused by the digital revolution differ from one another and whether and how differences in policy may exacerbate or mitigate the differences described above in approaches to AI.

The key words to describe the different aims pursued by governments in their approaches to the digital revolution, as previously mentioned, are control, promotion and protection. They are all features of the actual policies in the field. However, governments can privilege one more than the others when deciding which goals are to be preferred.

A special mention deserves the purpose of control: there would be no matter of concern if the digital revolution and the new technologies related to it would be under control of the producers or the users, the public powers, the societies or the individuals involved. Issues arise because of the lack of control over the most complex AI systems by any of these actors when it comes to HMI, as demonstrated with regard to the first and the second step of HMI's development. The fact is that technology is the result of a deliberate human decision, but its operability and diffusion is determined by the 'procreative prowess' of the technology itself.[55] The reaction of individuals and people to new technologies, their interaction with them and the way in which social practices and cultural reality change when they are entangled with media in the era of deep mediatization[56] are shaping the human evolution. The pervasiveness and ubiquitous nature of digital technology constantly remix the categories of everyday life in an unpredictable manner (the public and the private, the local and the global, the individual and the collective), while remaining invisible as far as their social functions are concerned.[57] The data protection regulations have been ineffective because they assume that controlling the behaviour of creators and producers of digital technologies will be sufficient to guarantee privacy. In this regard, the AI Act also will be inadequate to prevent harms coming from AI systems considered as mere product,[58] while digital technology coevolves with humans.[59]

---

[54] *Bradford*, The Brussels Effect: How the European Union Rules the World, 2020, passim.

[55] *Dennett*, From Bacteria to Bach and Back: The Evolution of Minds, 2017, passim.

[56] *Hepp*, Deep Mediatization, 2020, passim.

[57] *Deuze*, Media life, Media, Culture & Society 2011, Vol. 33 Iss. 1, 137 (137–148).

[58] *Mantelero/Fanucci*, Great ambitions. The international debate on AI regulation and the human rights in the prism of the Council of Europe's CAHAI, in: Czech et al. (eds.), European Yearbook on Human Rights, 2022, 225 (225–252).

[59] *Lee*, Are We Losing Control, in: Werthner/Prem/Lee/Ghezzi (eds.), Perspectives on Digital Humanism, 2022, 3 (3–7). Available at https://doi.org/10.1007/978-3-030-86144-5_1 (last accessed on: 31 August 2024).

Furthermore, the issues of controlling AI systems depend on the goals to be achieved. Humans are entitled to pursue their own objectives, while machines are not. When objectives are not completely clear for humans, machines are obliged to pursue them on our behalf. This uncertainty connected with the already described possible distortions coming from the HMI seems to be crucial to build AI systems of arbitrary intelligence that are provably beneficial to humans.[60]

Exploring the perspectives for sustainable innovation in the digital era, there is a need to understand whether policy goals driving government intervention in the sector vary significantly. In China, public interventions on AI and related technologies aim to control their operability and results as well as, through them, the population to ensure legal order and conforming social narratives. Digital surveillance is the terrain of the Chinese social credit system. In the US, the liberal dogma according to which the market sets the rule makes the promotion of technological development and the related business the principal purpose. AI systems, originally designed for military use, are exploited for government surveillance of civilians for security reasons, while the tech companies have commodified private human experience together with personal data for a new sort of capitalism.[61]

While China stresses the public purpose of people's control in regulating the digital revolution and the United States are reluctant to regulate the sector with the intent to promote technology development in order to boost the market-driven economy, the European Union seems more concerned about the impacts of AI models on fundamental rights. What seems to be a kind of protectionist policy promoted by European institutions, is the result of the European constitutional tradition, which prioritises human dignity, giving it precedence over liberty.[62] However, the EU AI Act mainly aims at market harmonisation and its risk-based structures provide only a still vague impact assessment in relation to the enjoyment of human rights by individuals.[63] The society itself and collective interests such as the functioning of democracy and the observance of the rule of law are not taken into account.[64] Nonetheless, European laws are proof of the efforts to prioritise the protection of EU citizens over the uncontrolled development and diffusion of digital technologies.

In short, in its digital policy, China gives priority to exerting control over the citizens, the US to promoting business and the economy, and the EU to protecting human rights.

---

[60] *Russell*, Artificial Intelligence and the Problem of Control, in: Werthner/Prem/Lee/Ghezzi (eds.), Perspectives on Digital Humanism, 2022, 19 (19–24).

[61] *Zuboff*, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, 2019, passim.

[62] *Pollicino*, I codici di condotta tra self-regulation e hard law: esiste davvero una terza via per la regolazione digitale? Il caso della strategia europea contro la disinformazione online, Rivista Trimestrale Di Diritto Pubblico 2022, Vol. 72 Iss. 4, 1049 (1049–1066).

[63] See FRIA above (I.).

[64] *Mantelero/Fanucci*, in: Czech et al., European Yearbook on Human Rights, 225.

## V. By Way of Conclusion

The Vienna Manifesto on Digital Humanism includes the principle that 'humans must shape technologies in accordance with their values and needs, instead of allowing technologies to shape humans'[65]. Unfortunately, that is what is happening in the so-called 'algorithmic regulation'.[66] The experience with algorithmic profiling in social media serves as a cautionary tale. Initially used for targeted advertising and personalised recommendations, these algorithms have been shown to exacerbate existing biases and create echo chambers, limiting exposure to diverse perspectives and nudging towards polarisation of societies and homogenization of individuals. In the current discussion on Digital Humanism, it is extremely relevant how every expert in dialogue with experts of other disciplines conceptualise humans, digital technologies and their interactions. AI systems, in particular CAs, are sociotechnical systems composed of physical things, simple or sophisticated, in interaction with humans as individuals or groups, whole societies, private and public organisations, institutions, together with contexts, conditions, and rules that are their frameworks.[67] Their hybrid nature intersects different fields and calls for innovative methodologies to foster creative dialectical collaboration between sciences.[68] While the components requiring a physical intervention are within the competence of scientific and engineering disciplines, the features of humans and the new dynamics of the HMI need humanities and social sciences in order to be interpreted.

### *1. The Political Arena*

In the political arena, lawmakers are reasserting control over digital sovereignty, aiming to contain the private powers of the big tech and to regulate the use of digital technologies with various purposes: control, promotion or protection. European institutions have dismissed the digital liberalism of the 2000s, embracing the new approach of digital constitutionalism.[69] China has created the Cyberspace Administration of China (CAC) in 2014,[70] with a broad wide investigating and regulating powers

---

[65] *Werthner et al.*, Vienna Manifesto on Digital Humanism, 2019. Available at https://caiml.org/dighum/dighum-manifesto/Vienna_Manifesto_on_Digital_Humanism_EN.pdf (last accessed on: 31 August 2024).

[66] *Cristianini/Scantamburlo*, On social machines for algorithmic regulation, AI & Society 2020, Vol. 35, 645 (645–662).

[67] *Veermas/Kroes/van de Poel/Franssen/Houkes*, A Philosophy of Technology: From Technical Artefacts to Sociotechnical Systems, 2011, 89 et seqq.

[68] *Schiaffonati*, Explorative Experiments and Digital Humanism: Adding an Epistemic Dimension to the Ethical Debate, in: Werthner/Prem/Lee/Ghezzi (eds.), Perspectives on Digital Humanism, 2022, 77 (77–82).

[69] *De Gregorio*, Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society, 2022, 273 et seqq.

[70] *Horsley*, Behind the Facade of China's Cyber Super-Regulator, Digichina 2022, available at https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/ (last accessed on: 31 August 2024).

for national security reasons. As part of the People's Republic of China propaganda system, this deliberative body manages online information content and law enforcement and drafts regulatory documents to ensure full control over data and narratives, actors and users in the digital sector[71] in order to maintain stability and people's best interest in accordance with communist ideology. The US established the National Security Commission on Artificial Intelligence[72] in 2018 'to comprehensively address the national security and defence needs of the United States' with the aim to protect the American leadership in AI, prioritising domestic interests and geopolitical superiority, preserving at the same time a hands-off regulatory environment driven by market innovation, neoliberal ideology, and individualistic values.[73]

In different ways, the EU, the US, and China are building legal fortresses to foster their values and prevent a 'digital colonization' from abroad. The fragmentation of the legal framework due to the differences in political purposes threatens to alienate the goal of any revolutionary innovation, which is to improve the human condition. The point is not that technology has to be human-centred, because humans are already at the centre of the AI system design.[74] Actually, individuals need to be protected from the unilateral asymmetries of private, public or technological powers, generated or amplified by the AI applications. To rebalance the ontological power asymmetries between humans and machines, the reinforcement of the users' position through the consent requirement or the right to withdraw is not effective. As demonstrated above, traditional legal instruments are only effective to a certain extent. The concerns about respect for fundamental rights cannot be completely alleviated by preliminary impact assessments or subsequent sanctions, depending both on the variations in the understanding of 'digital fundamental rights' across different jurisdictions.[75]

### *2. The Legal Arena*

In case of a revolution, the paradigm shift imposes to rethink the classical categories of law and adapt eventually old tools to the new context, but also to create new ones. The conceptualization of human rights at the end of the 18th century shaped the social and legal relationships between people. From that moment on the legal subject was conceived as autonomous and rational and the laws realised the Locke's philosophy

---

[71] *Chin/Li*, A Comparative Analysis of Cyber Sovereignty Policies in China and the EU, SSRN 2021, 1, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3900752 (last accessed on: 31 August 2024).

[72] The National Security Commission on Artificial Intelligence (NSCAI) was established by Sec. 1051 of the National Defense Authorization Act for Fiscal Year, 2019.

[73] *Hine/Floridi*, Artificial Intelligence with American Values and Chinese Characteristics: A Comparative Analysis of American and Chinese Governmental AI Policies, AI & Society 2024, Vol. 39, 257 (257–278).

[74] *Bertolaso/Capone/Rodríguez-Lluesma*, Digital Humanism. A Human-Centric Approach to Digital Technologies, 2022, 1–9.

[75] *Pollicino*, Protection, 147.

of liberal individualism, based on the idea that all human beings are by nature free and endowed with the same inalienable rights.[76] The principle of equality imposed to the public institutions the sameness treatment for all, except protected categories or people in particular conditions, minors, disabled people etc. However, the formal equality principle has proven inadequate to address power imbalances between individuals and public or private powerful actors.[77] The state non-intervention, in particular in the American legal culture, has facilitated the exploitation of persons' weakness by superior private entities. As explained above, the same is happening with regard to the digital revolution with the difference that risks and harms are amplified and unpredictable. Digital technologies and AI systems are shaping not only the human environment, but the entire humanity at the individual and societal level.

As the mass production augmented, oligopolistic strategies and the power imbalance reduced the possibility for their counterparties to resist unfair practices. Thereby, governments intervened to assure competition between actors and protection of the weakest parties in the marketplace. Along with the notion of consumer, as a natural person who purchases goods and services for personal use, consumer law deals with actions and remedies, rights and duties, to ensure the fairness of commercial practices and the rebalance of the powers through consumer empowerment and information. In recent times, the notion of the 'average consumer' is object of revisitation by legal scholars, substituted by the 'vulnerable consumer'. In consumer law, digital vulnerability describes 'a universal state of defencelessness and susceptibility to (the exploitation of) power imbalances that are the result of increasing automation of commerce, datafied consumer-seller relations, and the very architecture of digital marketplace'[78].

### *3. The Concept of Vulnerability in Consumer Law*

The concept of vulnerability is intrinsic to the human condition. In consumer law, according to Art. 5 para. 3 of the Unfair Commercial Practices Directive the vulnerable consumer belongs to a 'clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity in a way which the trader could reasonably be expected to foresee'. However, vulnerability is not only caused by internal factors. External factors could originate, sustain, and even reinforce vulnerabilities.[79] In data

[76] *Seliger*, The Liberal Politics of John Locke, 2nd ed., 2019; *Turner*, Individualism, Capitalism and the Dominant Culture: A Note on the Debate, The Australian and New Zealand Journal of Sociology 1988, Vol. 24 Iss. 1, 47 (47–64).

[77] *Fineman*, Yale Journal of Law & Feminism 2008, Vol. 20 Iss. 1.

[78] *Helberger/Sax/Strycharz/Micklitz*, Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability, Journal of Consumer Policy 2022, Vol. 45, 175 (175–200).

[79] *Peroni/Timmers*, Vulnerable groups: The promise of an emerging concept in European human rights convention law, International Journal of Constitutional Law 2013, Vol. 11 Iss. 4, 1056 (1056–1085).

protection law, special categories of sensitive data are protected in a more stringent way, revealing the vulnerability of correspondent data subjects.[80]

The AI Act refers to the concept of vulnerability in two ways, revealing how the term is still vague and ambiguous.[81] On the one hand, Art. 5 para. 1 lit. b AI Act uses the limited extent of the situational vulnerability, restricting the reference to the 'vulnerabilities of a person or a specific group of persons due to their age, disability or a specific social or economic situation' in order to prohibit their exploitation; similarly, Art. 7 para. 2 lit. h AI Act says 'the persons who are potentially harmed or suffer an adverse impact are in a vulnerable position in relation to the deployer of an AI system, in particular due to status, authority, knowledge, economic or social circumstances, or age' and Art. 9 para. 9 AI Act refers to 'persons under the age of 18 and, as appropriate, other vulnerable groups' (references also in Art. 60 para. 4 lit. g, Art. 79 para. 2, Art. 95 para. 2 lit. e AI Act). On the other hand, Art. 15 para. 5 AI Act states that AI systems can also be vulnerable to attempts by third persons to alter their use, outputs or performance.

### *4. The Concept of Digital Vulnerability as a New Legal Macro-Category in HMI*

The misuse of the word 'vulnerability' by the European legislator is not surprising, considering the anthropomorphization of AI operated by AI developers, computer scientists, designers, and programmers. The employ of terms typically used to describe human skills and capacities focuses on alleged similarities between humans and machines, in particular in brain inspired AI. This anthropomorphism has epistemological and ethical consequences[82] and is to be avoided at all costs. The vulnerability of an AI system can be considered only when it implies harm and rights' violation of the humans who are using or depend on that system, so that vulnerability as well as intelligence are exclusively human peculiarities.

Facing the digital revolution, all humans are vulnerable to the pervasiveness of and the dependence from technology. Ethics science is of pivotal importance to educate designers, producers and deployers of AI systems. AI systems themselves cannot indeed be educated to ethics and their deterministic approach, the way in which they nudge humans towards unpredictable paths, puts mankind and its societal structures in danger. *Stuart Russel's* proposal to design machines to be inherently uncertain about the humans' preferences they are required to satisfy, theorises humble and altruistic machines, committed to pursue humans' objectives, not theirs. In the inten-

---

[80] *Malgieri/Niklas*, Vulnerable data subjects, Computer Law & Security Review 2020, Vol. 37 article no. 105415, 1 (1–16).

[81] *Schroeder/Gefenas*, Vulnerability: Too Vague and Too Broad? Cambridge Quarterly of Healthcare Ethics 2009, Vol. 18 Iss. 2, 113 (113–121).

[82] *Salles/Evers/Farisco*, Anthropomorphism in AI, American Journal of Bioethics Neuroscience 2020, Vol. 11 Iss. 2, 88 (88–95).

tion of the author, this might result in a new foundation of the HMI, provably deferential and beneficial.[83]

However, in the present digitally boosted, multiple-choice society people get overwhelmed with an excessively large number of options.[84] The choice overload leads to decision fatigue and increases the frustration due to the missed opportunities.[85] In this context, the asymmetry on the data management between humans and machines creates the conditions for exacerbating the susceptibility to manipulative persuasion and the predisposition to decision delegation. The loss of control over social narratives and the deprivation of the individual self-determination in the presumption of the maximal freedom of choice[86] are the grounds of human vulnerability in interaction with AI.

The concept of vulnerability is a wide concept intrinsic to human beings, useful to describe at the same time the universal and the situational condition of individuals, groups of individuals up to the society per se. In particular, the Luna's theory of layers[87] overcomes through an intersectional approach[88] the tension between the universalistic and the particularistic character of vulnerability, explaining how its features may vary from one individual to another, having different causal factors and degrees of severity. In this regard, it seems to offer the right conceptual pivot around which to build a common and global regulation on digital law. The concept of digital vulnerability fits better with the multidimensional and multi-layered digital revolution. It is consistent with the present movement towards a digital constitutionalism,[89] stressing the backgrounds of the fundamental human rights shared globally at an international level. Furthermore, the idea of vulnerability has a relational nature so that it is very suitable to digital law, where the very risks and threats coming from advanced AI systems are indeed connected with the HMI.

To conclude, there is the need for a common guiding legal principle with educational intent in order to make people aware of the risk involved not only in using AI, but also in interacting with it. The law should be given credit for this educational function.

The perception of human vulnerability, precisely because it is ontologically intrinsic to mortal nature, is evident in relations between humans as moral agents. In con-

---

[83] *Russel*, Human Compatible. Artificial Intelligence and the Problem of Control, 2019, passim.

[84] *Breedveld/Broek*, De meerkeuzemaatschappij: facetten van de temporele organisatie van verplichtingen en voorzieningen, 2003, passim.

[85] *Schwartz*, The Paradox of Choice. Why More Is Less, 2004, passim.

[86] *Bareis/Katzenbach*, Talking AI into Being: The Narratives and Imaginaries of National AI Strategies and Their Performative Politics, Science, Technology, & Human Values 2021, Vol. 47 Iss. 5, 855 (855–881).

[87] *Luna*, Elucidating the Concept of Vulnerability: Layers Not Labels, International Journal of Feminist Approaches to Bioethics 2009, Vol. 2 Iss. 1, 121 (121–139); *Luna*, Identifying and evaluating layers of vulnerability – a way forward, Developing world bioethics 2019, Vol. 19 Iss. 2, 86 (86–95).

[88] *Bond*, Global Intersectionality and Contemporary Human Rights, 2021, 20 et seqq.

[89] *Pollicino*, Protection, 200 et seqq.; *De Gregorio*, Constitutionalism, 277 et seqq.

trast, HMI is still uncharted territory. The first step of HMI has already shown how dangerous and hidden the threats to the personal and social dynamics of identity construction can be. The second step, as it opens up new horizons and applications, could be even more dangerous. On the one hand, the individual experiences a certain empowerment; on the other hand, the individual's vulnerability is exacerbated by a predisposition to delegate decisions and give space to nudges. The solution might be to always have a human in the loop, but that is not enough.

The introduction of the principle of digital vulnerability in the European and international context could act as a catalyst for global regulatory initiatives. Like the consumer-professional imbalance recognised in consumer law, there is an imbalance of power and capabilities between humans and machines. Therefore, declaring the ontological vulnerability of humans in any interaction with AI, making the concept of digital vulnerability a new macro-category in private law, and interpreting existing norms or drafting future ones on its basis could be the right legal tool to lay the foundation for a global digital law. The concept of vulnerability lends itself to bridging the world's different philosophical and religious cultures, as both philosophy and religion are responses to the inherent vulnerability common to all beings.[90] Moreover, at a national level, the concept of digital vulnerability would allow countries to address the three approaches described above – control, promotion and protection –, harmonising them towards a digital humanism.

[90] *Tham*, The Principle of Vulnerability: Meeting Ground of Six Religions, in: Tham/Garcia/Miranda (eds.), Religious Perspectives on Human Vulnerability in Bioethics, 2014, 1 (1–10).

# Verzeichnis der Autorinnen und Autoren

Univ.-Prof. Dr. *Philipp Anzenberger*
Universitätsprofessor am Institut für Zivilgerichtliches Verfahren an der Leopold-Franzens-Universität Innsbruck.

Assoz.-Prof. Priv.-Doz. Dr. *Manfred Büchele*
Assoziierter Professor am Institut für Unternehmens- und Steuerrecht der Leopold-Franzens-Universität Innsbruck.

Prof. Dr. *Amalia Diurni*
Professore Ordinario am Dipartimento di Management e Diritto der Università di Roma Tor Vergata.

Dott. *Stefano Gatti*
Ricercatore am Dipartimento di Scienze Giuridiche der Università di Verona.

Univ.-Prof. Dr. *Severin Glaser*
Universitätsprofessor am Institut für Strafrecht, Strafprozessrecht und Kriminologie der Leopold-Franzens-Universität Innsbruck.

Dr. *Günther Hauss*
Senior Supervisor im Single Supervisory Mechanism bei der Europäischen Zentralbank.

*Sarah Hinck*
Wissenschaftliche Mitarbeiterin an der Juristischen Fakultät der Heinrich-Heine-Universität Düsseldorf.

OStA DDr. *Konrad Kmetic*
Oberstaatsanwalt und delegierter Europäischer Staatsanwalt in Österreich.

Univ.-Prof. Dr. *Bernhard A. Koch*, LL.M. (Michigan)
Universitätsprofessor am Institut für Zivilrecht der Leopold-Franzens-Universität Innsbruck.

Prof. *Lorenzo Picotti*
Già Professore Ordinario (im Ruhestand) am Dipartimento di Scienze Giuridiche der Università di Verona.

Prof. Dr. *Rupprecht Podszun*
Inhaber des Lehrstuhls für Bürgerliches Recht, deutsches und europäisches Wettbewerbsrecht an der Heinrich-Heine-Universität Düsseldorf und Direktor des Instituts für Kartellrecht.

em. o. Univ.-Prof. Dr. *Klaus Schwaighofer*
Emeritus am Institut für Strafrecht, Strafprozessrecht und Kriminologie der Leopold-Franzens-Universität Innsbruck.

Prof. Dr. *Stefano Troiano*, Ph.D.
Professore Ordinario am Dipartimento di Scienze Giuridiche der Università di Verona.

Univ.-Prof. Dr. *Andreas Venier*
Universitätsprofessor und Leiter des Instituts für Strafrecht, Strafprozessrecht und Kriminologie der Leopold-Franzens-Universität Innsbruck.