



UNIVERSITY OF AMSTERDAM
Institute for Information Law



Information Law and the Digital Transformation of the University

Part I. Digital Sovereignty

Information Law and the Digital Transformation of the University

Part I. Digital Sovereignty

Authors: Arlette Meiring, Svetlana Yakovleva, Kristina Irion, Joris van Hoboken and Mireille van Eechoud

Citation: Institute for Information Law (2023). Information Law and the Digital Transformation of the University. Part I. Digital Sovereignty. Amsterdam: September 2023.

<https://www.ivir.nl/part-i-digital-sovereignty/>

Funding: This report was commissioned by the Executive Board of the University of Amsterdam.

The opinions expressed in this work reflect the authors' own views and not those of the commissioning organisation. The research for this report has been conducted in full compliance with the Netherlands Code for Conduct for Research Integrity (2018).

Amsterdam, 15 September 2023



University of Amsterdam
Institute for Information Law
P.O. Box 15514
1001 NA Amsterdam
The Netherlands
Website: <https://www.ivir.nl/>



This report is covered by a [Creative Commons Attribution 4.0 International Licence](https://creativecommons.org/licenses/by/4.0/).

Executive summary

As in other sectors of society, the digital transformation of universities is driven to a large extent by the adoption of technologies produced in (global) markets. Many digital infrastructures and services used in the university sector are supplied by commercial entities, as a result of which the digital design of public universities is increasingly shaped by the logic and values of the market. The concentration of digital infrastructures, and the data generated and stored therein, in the hands of powerful corporate entities bears the risk that public values on which universities are founded will erode.

Recently, universities have become vocal about their quest for “digital sovereignty” in order to safeguard academic values and preserve the future of universities as independent public knowledge institutions in the digital age. This call is a response both to the growing power of technology companies and to the avalanche of new EU legislation that targets digital services and data governance. The autonomy of universities is in some parts of Europe under threat from serious political interference; that is however not an issue addressed in this project.

Against this background, this report aims to achieve two objectives. First, it untangles and interprets the concept of digital sovereignty as applied to the university context, by connecting it to academic values and the public mission of universities. Second, it analyses recent and emerging regulation at the level of the European Union targeting digital services and data that (directly or indirectly) affects universities and academics, through the lense of digital sovereignty. This report is part of the research project “Information Law and the Digital Transformation of the University” commissioned by the Executive Board of the University of Amsterdam. The project aims to clarify digital sovereignty- and data access-needs of universities in light of their public mission. Part 2 focuses on researcher access to data especially in light of new EU legislation.

Digital sovereignty in the university context: findings and recommendations

The articulation of a framework for digital sovereignty specific to universities can be summed up in the following findings.

Findings

- **The concept of digital sovereignty as applied to universities and academics**

Both universities (as institutions) and academics (individually or collectively) can justifiably make ‘claims’ for digital sovereignty in the interest of preserving and promoting academic values in the digital academic sphere. Digital sovereignty claims arise from, and are defined by, threats to academic values stemming from the commercial supply of digital services and infrastructures that supersede universities’ and academics’ ability to take autonomous decisions and actions regarding digital infrastructures and data.

- **Digitalisation and commercialisation of the university sector**

Society expects that universities utilise the potential of data and digital infrastructures for scientific advancement. Due to universities’ increasing reliance on commercial suppliers, however, the external influence on universities’ digital designs and academic practices grows. This trend has given rise to concerns about techno-commercial logics ‘crowding out’ academic values and the deliberate extraction of personal and other data from universities’ digital environment for suppliers’ economic gains.

- **Digital sovereignty necessary to safeguard academic values in the digital age**
Three ‘core’ values have traditionally guided public universities’ commitments and activities: scientific advancement, academic freedom and institutional autonomy. These core academic values remain important in the digital world. Digital sovereignty is a necessary precondition for universities to realise these academic values and to uphold their public function as autonomous knowledge producers in the digital era.
- **Specific needs in the university context**
Universities’ digital sovereignty needs (and therefore claims) concern digital infrastructures and data. Regarding digital infrastructures, the claims typically relate to addressing (1) power asymmetries and high barriers to switching between suppliers, (2) suppliers forcing deals through the bundling of services, and (3) the subtle capture of universities’ digital environments by techno-commercial affordances. Turning to data, universities are mainly concerned about (4) the capture and extraction of (personal) data for commercial ends, (5) the public sharing of research data on commercial demand, while (6) access to privately held data for scientific research remains highly exceptional. While some of these claims can be addressed with better procurement strategies, universities’ capacity is limited in highly concentrated markets and in situations where information and power asymmetries are prominent, for instance vis-à-vis online platforms.

Recommendations

In light of the findings, the advice to universities is to:

- **Develop a procurement framework that integrates the safeguarding of academic values;** tools can include lock-in risk assessments, data protection impact assessments and compliance audits;
- **Produce shared knowledge about legal and technical assessments of frequently procured digital services and infrastructures and team up as a sector** to increase negotiation power vis-à-vis large suppliers of digital services and infrastructures; and
- **Promote services and technologies developed with academic values and the public interest in mind** and diversify the digital portfolio where possible.

EU law and digital policy: findings and recommendations

An important venue for putting the freedom of sciences and the right to research centre stage is EU law and policy, which exercises increasing influence on the conditions under which universities and academics carry out public interest-oriented scientific research. There is a growing body of (upcoming) legislation relevant to universities (e.g. Open Data Directive, Data Governance Act, Data Act, Digital Services Act and AI Act). An analysis produces the following key findings:

Findings

- **Legal uncertainty and complexity**
It follows from the legal analysis that there is no harmonised EU definition of ‘scientific research’, and that its meaning and scope varies by legislative instrument. The overall picture emerges that the piecemeal recognition of scientific research in EU digital and data legislation makes legal compliance for universities and academic researchers unnecessarily complex.
- **Increasing administrative and financial burdens**

European universities fully support the objectives underpinning the EU's Open Science Policy, but more attention should be paid – by law- and policymakers and research funders – to the administrative and financial burden that comes with their legal obligation to make research data resulting from publicly funded research available for re-use. Scientific research activities are also affected by a surge in EU digital and data legislation adopted under the EU's digital strategy. They rarely however enjoy a particular status. One rare example is the text- and datamining provision of the Copyright in the Digital Single Market Directive. In a few other cases, public interest-driven research has been implicitly exempted from legal obligations on the ground that it is not considered an economic activity. Sometimes, legislative instruments confer helpful privileges or exceptions for scientific research (subject to specific legal requirements).

Recommendations

In light of the findings, this report recommends law- and policymakers to:

- **Give broad recognition to scientific freedom as a cross-cutting policy issue** that transcends the EU's Open Science Policy and elevates the objectives of scientific research throughout the EU's policy cycle;
- **Adopt a consistent notion and definition of scientific research across legislation** which emphasises the public-interest nature of scientific research and its adherence to recognised ethical standards of scientific research and open science;
- **Continually assess and address the internal coherence** of EU data and digital legislation from the perspective of promoting scientific research.

TABLE OF CONTENTS

| | |
|---|-----------|
| Executive summary | 2 |
| Introduction | 7 |
| 1. Digital sovereignty | 9 |
| 1.1 EU discourse on digital sovereignty..... | 9 |
| 1.2 Conceptualising digital sovereignty | 10 |
| 1.2.1 Dimensions of digital sovereignty | 10 |
| 1.2.2 Actors of digital sovereignty..... | 11 |
| 1.2.3 Meaning of digital sovereignty | 14 |
| 1.3 Digital sovereignty in the university sector | 14 |
| 1.3.1 Digitalisation and datafication of universities..... | 15 |
| 1.3.2 Commercialisation of the digital academic sphere..... | 16 |
| 1.4 A model for digital sovereignty in the university context..... | 19 |
| 2. Normative underpinnings of digital sovereignty claims in the university context | 21 |
| 2.1 Universities’ role in society | 21 |
| 2.2 Academic values and their legal articulation | 23 |
| 2.2.1 Scientific advancement..... | 24 |
| 2.2.2 Academic freedom..... | 25 |
| 2.2.3 Institutional autonomy | 30 |
| 2.2.4 Protection and promotion of academic values..... | 32 |
| 2.3 Academic values and digital sovereignty | 32 |
| 3. Digital sovereignty claims in the university context | 34 |
| 3.1 Generic and specific digital sovereignty claims | 34 |
| 3.2 Claims relating to digital technologies and infrastructures | 36 |
| 3.2.1 Concentrated markets and technology-and-vendor lock-ins | 36 |
| 3.2.2 Bundling of read-and-publish services and data analytics services | 38 |
| 3.2.3 Commercial influence on research, education and university decision-making..... | 40 |
| 3.3 Claims relating to data | 41 |
| 3.3.1 Large-scale (meta)data collection and exploitation..... | 42 |
| 3.3.2 Limited access to data for research purposes | 43 |
| 3.3.3 Instrumentalisation of publicly-funded research data for commercial gain | 43 |
| 3.4 Universities’ agency to address digital sovereignty claims and its limits..... | 45 |
| 4. Impact of EU law and policy on digital sovereignty in the university context | 47 |
| 4.1 EU policies for the digital age | 47 |
| 4.2 Rights and obligations of universities and researchers under EU digital/data law | 49 |
| 4.2.1 Use of digital infrastructures and services (infrastructure input)..... | 49 |
| 4.2.2 Provision of digital infrastructures and services (infrastructure output)..... | 51 |
| 4.2.3 Use of data for research purposes (data input) | 52 |
| 4.2.4 Provision of research data (data output) | 58 |
| 4.2.5 Connection with digital sovereignty..... | 62 |
| 4.3 Recognition of universities’ interests and academic values in EU law and policy..... | 63 |
| 4.3.1 The notion of “scientific research” in EU legislation | 64 |
| 4.3.2 Targeted EU legislative intervention?..... | 65 |
| 4.3.3 Anchoring scientific research into EU law | 66 |
| Conclusions and recommendations | 68 |
| Bibliography | 72 |

Introduction

In recent decades, digital infrastructures have become a key resource enabling research and education at universities.¹ Universities, especially through their computer science departments, have played a major role in the advancement of information technologies and the creation of shared digital infrastructures for scientific research. Nonetheless, universities have become by and large reactive in shaping the governance of the digital infrastructures they rely on for academic research, educational programmes and institutional facilities. To varying degrees universities have been outsourcing digital infrastructures and services provision to commercial suppliers.² Together with broader development in digital markets, this has contributed to a concentration of data infrastructures in the hands of a few powerful technology companies, which wield quite some influence over universities' digital design.

Scientific advancement, academic freedom and institutional autonomy are important public values that should be preserved in the course of universities' digital transformation. Recently, universities have become increasingly vocal about their quest for "digital sovereignty" in order to safeguard these values and the future of universities as independent public knowledge institutions more generally.³ In 2019, for example, leading academics published an opinion in a Dutch newspaper, signed by 14 rectors of Dutch universities, in which they called for a better alignment of the use of commercial digital platforms with public values central to higher education and academic research.⁴ The University of Amsterdam has also declared digital sovereignty as a "core value" of its Digital Agenda, and SURF, the Dutch collaborative organisation for IT in research and education, has identified it as a topic of special attention for 2022-2027.⁵ However, when academic digital sovereignty is called for, this notion is often not well explained, which can undermine the credibility of universities' claims.

The objective of this report is to develop an account of digital sovereignty tailored to the university sector that can be used by universities and academics to advance their public missions in the digital age. In doing so, it specifically focuses on research activities oriented toward scientific advancement in the public interest. The branches of education and institutional governance are discussed where necessary. Aside from interrogating universities' relationship with providers of digital infrastructures and services, this report also looks at the current and emerging regulatory environment impacting digital sovereignty of universities.

The report is the first of several research outputs that have been produced as part of a broader study into the challenges associated with the digital transformation of universities that the Executive Board of the University of Amsterdam has commissioned from the Institute for Information Law (IViR). The other outputs include a report on access to data for research ("Part II"),⁶ an expert memorandum on the General Data Protection Regulation as a means to protect universities' digital sovereignty,⁷ and a number of factsheets providing information on selected instruments of EU digital and data law.

Significantly, it must be emphasised that the digitalisation and datafication of universities is not problematic per se. Digitalisation has enabled universities to introduce innovative methods of research, enhance access to and findability of scientific and cultural heritage, and facilitate access to knowledge.

¹ In this report, the terms "university", "academic institution" and "higher education institution" are used interchangeably and refer to centres of post-secondary scientific research and education.

² In the context of this report, we refer to digital infrastructures as socio-material artefacts consisting of both technical/material components (such as cables, hardware devices, data centres) and organisational/socio-technical components (e.g., settings, standards, governance structures, relationships and processes that contribute to the functioning of an information system). See e.g., Ferrari 2023, p. 23 and Henfridsson and Bygstad 2013, p. 908-909. For a more technical/material interpretation, see Constantinides, Henfridsson and Parker 2018, pp. 381-400, as endorsed Van Dijk, Nieborg and Poell 2019, p. 17-18.

³ LERU Data Statement 2021; see also the speech by Karen Maex, former Rector Magnificus of the University of Amsterdam, on the Dies Natalis of the university in January 2021 titled 'Protect independent and public knowledge'.

⁴ Maex et al, 'Digitalisering bedreigt onze universiteit. Het is tijd om een grens te trekken', de Volkskrant 22 December 2019.

⁵ Digitale Agenda UvA 2022, p. 24; SURF Strategy 2022-2027, p. 7.

⁶ Institute for Information Law, 'Information Law and the Digital Transformation of the University: Digital Sovereignty, Data Governance and Researchers' Access to Data – Part II. Access to Data for Research', 2023.

⁷ A. Roosendaal, 'The GDPR as a means to protect digital sovereignty of universities', 2023.

Universities are moreover expected by society to utilise the potential of data and digital infrastructures. Issues arise, however, when digital services and service providers override or undermine the public-value orientation of universities. The main challenge is to prevent that the digital transformation – if not carefully governed – diverts universities and academics from their core missions and orientation toward public values by reducing their institutional autonomy, academic freedom and, by implication, their ability to independently pursue strategic goals. Paying critical attention to the protection of universities’ and academics’ digital sovereignty can be a means to mitigate the risks of the digital age.

Against this background, the central research question this report aims to answer is: *What does digital sovereignty mean within the university and scientific research context, how can it be leveraged to defend and promote academic values, and what is the role of EU law and policy in this regard?* To produce this report, a combination of research methods have been used, namely qualitative research, normative research and legal analysis. The empirical basis builds on documents and multidisciplinary literature on digitalisation and concentration in digital markets, conceptualisation of digital sovereignty, the role of universities and academic values, and relevant legal and policy developments in the digital domain. This report is situated in the European Union (EU) context but uses many examples from the Dutch university landscape. The preliminary research findings were discussed during an expert workshop held on 26 January 2023 together with academics, stakeholders from the university sector, and policymakers from the Dutch government and the EU.

The report is structured as follows: Chapter 1 first aims to demystify the fuzzy notion of digital sovereignty by identifying its dimensions and actors involved, on the basis of which it develops a model of digital sovereignty ‘claims’ for the university sector. Chapter 2 then gives an account of the normative values that universities embody and clarifies how these values underpin the digital sovereignty claims made by universities and academics. After that, Chapter 3 provides an overview of specific digital sovereignty claims made in the university sector in relation to digital infrastructures and data. Chapter 4 explores the impact of EU law and digital policy on universities and academics and assesses whether it enhances digital sovereignty in the university context or is rather impairing. The report concludes with a summary of conceptual findings and a set of recommendations addressed to universities and academics as well as research funding organisations and policymakers at EU and Member States’ levels on how to prevent and remedy the (further) erosion of digital sovereignty in the university sector and on how to operationalise the concept in practice.

1. Digital sovereignty

Digital sovereignty is a fluid and socially constructed concept that encompasses different types of claims depending on the specific context and actors involved. Common themes used in the public discourse on digital sovereignty are the ‘control’ or ‘self-determination’ over the design and use of digital technologies and infrastructures, and over the data generated and stored in those infrastructures.⁸ The European policy-oriented discourse on digital sovereignty forms the starting point of this Chapter’s exploration of the notion. The insights into how digital sovereignty is generally interpreted and justified are then used to give meaning to the concept in the specific context of universities. A better understanding of digital sovereignty will ultimately contribute to its effective use in safeguarding academic values in the digital realm as discussed in the following chapters.

1.1 EU discourse on digital sovereignty

The notion of “digital sovereignty” recently gained traction in the policy discourse at the level of the EU.⁹ There, digital sovereignty is used as an umbrella term to refer to the EU’s strategic policy objective to address a range of challenges to the European economy and society associated with the use of digital technologies and data. One of the leitmotifs of the discussion is the necessity to address dependencies on digital services, infrastructures and components from commercial suppliers, foreign or domestic. This has become a point of concern, as these companies lack democratic legitimacy and accountability and do often not fully safeguard European values.¹⁰ Another argument for digital sovereignty is the urgency for regulators, organisations and individuals alike to regain control over data in order to reap the benefits of data-driven technologies while ensuring respect for European rules and values.¹¹ Relatedly, there is the competitive aim of the EU and its Members States to build “strategic autonomy” vis-à-vis other states and large foreign technology companies. Digital sovereignty in this context is considered as an essential component of strategic autonomy in the digital realm,¹² which can be achieved by actively asserting the power to regulate the digital sphere and by fostering domestic digital infrastructures, core components such as chips, and emerging technologies such as artificial intelligence and quantum computing.¹³ EU policies aimed at enhancing strategic autonomy in the digital realm both have internal and external effects and harness a combination of public-interest regulation and industrial policies to promote key digital industries.¹⁴ In sum, European digital sovereignty both has defensive and offensive rationales.

⁸ See e.g., Stolwijk et al 2022; Moerel and Timmers 2020, p. 6; Fleming 2021; Seifried et al 2021, p. 6-7. For an overview of definitions in policy reports, documents of other stakeholders and academic research in German, see Seifried et al 2021, p. 61-64.

⁹ See e.g., European Commission, ‘A Europe Fit for the Digital Age’ (webpage), <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en>; European Commission, ‘Europe: the Keys to Sovereignty’ (news webpage), <https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en>; Madiaga (European Parliamentary Research Service) 2020; Berlin Declaration on Digital Society and Value-Based Digital Government 2020. Digital sovereignty is also increasingly discussed at the level of individual EU Member States, most notably in Germany but also in other countries. See Lambach and Oppermann 2022; Seifried et al 2021, p. 6-7; Thieulin 2019 (France), p. 18.

¹⁰ Pohle and Tiel 2020, p. 2, 6-7.

¹¹ In particular; compliance with EU personal data protection law. European Commission, A European strategy for data, COM/2020/66 final, para 3 and 5B.

¹² Soare 2022, p. 23.

¹³ In the context of the European digital strategy, “strategic autonomy” includes: the EU’s law-making power vis-à-vis other states and large (foreign) technology companies; the EU’s geopolitical power and competition; and the EU’s ability to decide and act upon the essential aspects of the European long-term future in the economy, society and institutions. See: Borell 2020; Michel 2021; Grevi 2019; Christakis 2020, p. 48; Timmers 2019, p. 636. It is sometimes also referred to as “strategic sovereignty”, see Leonard and Shapiro 2019.

¹⁴ Bendiek and Stürzer 2022; French and German Governments 2019 (Franco-German Manifesto).

1.2 Conceptualising digital sovereignty

It follows from the EU’s discourse as well as from some EU Member States’ discourses¹⁵ that the notion of “digital sovereignty” is oftentimes used as a discursive tool to support a wide variety of narratives and objectives. Observing these different contexts, this report prefers to speak about digital sovereignty claims (which underpin digital sovereignty needs) rather than digital sovereignty as a fixed concept that can be exhaustively defined. This approach allows us to delineate between the different dimensions of digital sovereignty and actors making claims for digital sovereignty. Deconstructing the notion of digital sovereignty into categories of claims allows us to give it a more precise meaning in the university context and to explore the foundations for universities’ own digital sovereignty discourse.

1.2.1 *Dimensions of digital sovereignty*

As noted above, digital sovereignty is a multi-dimensional concept closely associated with retaining control or agency in the digital environment. While the term digital sovereignty is quite recent, the phenomena that brought it into existence are not new. Similar concepts, such as “technological sovereignty” and “data sovereignty”, have also been used in European discourse to inform initiatives and policies in response to threats caused by the digital transformation.

“Technological sovereignty” generally refers to the power of states or communities to make decisions on how technologies are developed, used, accessed, distributed and consumed,¹⁶ and to the strategic independence of organisations from foreign technology suppliers.¹⁷ In the past, the technological sovereignty narrative empowered open software communities¹⁸ and underlay projects such as decentralised networks, encryption and digital alternative currencies.¹⁹ In European discourse, technological sovereignty has both been used as a synonym²⁰ and a subset of digital sovereignty.²¹

“Data sovereignty” is a shorthand for the ability to exercise control over the collection, access to, use and transfer of data as well as the ability to subject data to the data governance structures of a certain community or jurisdiction.²² EU regulators have used the term data sovereignty to refer to individuals’ and businesses’ ability to exercise control over their personal and non-personal data and to maintain trust in data sharing services.²³ Data sovereignty has also been used in the context of collective data governance frameworks, such as data cooperatives in smart cities.²⁴

It can be argued that technological sovereignty and data sovereignty both fall under the umbrella of the “digital sovereignty”, as they essentially emphasise its different aspects/dimensions. In this report, we broadly distinguish between claims for sovereignty in relation to (1) digital technologies and

¹⁵ E.g., in Germany, see Lambach and Oppermann 2022.

¹⁶ Padilla 2017, p. 5.

¹⁷ Seifried et al 2021, p. 12.

¹⁸ Riemens 2014, p. 29; Haché 2017, p. 165.

¹⁹ Riemens, p. 31.

²⁰ See for example the State of the Union Address by President von der Leyen 15 September 2021; see also Madiega (European Parliamentary Research Service) 2020, p. 1; Pohle and Tiel 2020.

²¹ See e.g., the European Data Strategy, in which technological sovereignty is considered necessary for the well-functioning of the European data economy: European Commission, A European strategy for data, COM(2020) 66 final, paras. 3 and 5B.

²² European Commission Staff Working Document Impact Assessment Accompanying Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, 13 September 2017, SWD(2017) 304 final; see also Irion 2013, and Seifried et al 2021, p. 12-13.

²³ European Commission Staff Working Document Impact Assessment Report accompanying Proposal for a Regulation on European Data Governance (Data Governance Act), 12 November 2020, SWD(2020) 295 final.

²⁴ Calzada 2021.

infrastructures, and (2) the data generated by and/or stored in those technologies and infrastructures. This distinction will inform further discussion in the report (Image 1).²⁵



Image 1. Dimensions of digital sovereignty/categories of digital sovereignty claims

1.2.2 Actors of digital sovereignty

Digital sovereignty is not exclusively the domain of states and the EU. In political, societal and academic debates, digital sovereignty is increasingly asserted by other, non-state actors such as organisations (groups or communities) and individuals.²⁶ Some academics argue that digital sovereignty clearly departs from the traditional attributes of ‘sovereignty’, both from the state-centric approach and from the prerequisite that sovereignty must be defined by a fixed geography.²⁷ The approach taken in this report is that digital sovereignty can indeed be asserted by different types of actors.²⁸ We distinguish between three types of such actors. First, states, state-like unions and local governments; second, private sector organisations, communities and groups; and third, individuals in their different roles in society.²⁹

It should be noted that the beneficiary of digital sovereignty claims does not always have to coincide with the actor making the claims. For example, individuals’ claims for digital sovereignty in their capacity of consumers of digital technology are effectuated by EU policymakers when passing consumer legislation (e.g., by giving them actionable remedies). The recently adopted Data Governance Act and the forthcoming Data Act, for instance, seek to strengthen the rights of data users and promote data sharing.³⁰ This does not mean that consumers and data users are merely passive beneficiaries; they may collectively try to influence policymakers and call for the legal protection of their claims. Overall, however, the distinction between actors that make claims about digital sovereignty and actors who benefit from such claims helps to structure the discussion.

Digital sovereignty claims by states and state-like unions

²⁵ The distinction between digital technologies, infrastructure, systems and data has also been made in literature, see e.g., the German Federal Ministry for Economic Affairs and Energy 2019, p. 7 with reference to the definition used by the Digital Summit Focus Group ‘digital sovereignty in a Connected Economy’; see also Moerel and Timmers 2020, p. 8; compare also EIT Digital 2020 (“digital infrastructure” and “data governance”).

²⁶ For academic discussion supporting this approach, see e.g., Roberts et al 2021, p. 2, 7; Floridi 2020, p. 371, 377.

²⁷ Roberts et al, p. 7.

²⁸ Ibid.

²⁹ Compare Seifried et al 2021, p. 11; European Digital SME Alliance 2021; Schulz et al 2022, p. 6-7 (distinguishing between micro- meso- and macro-levels of digital sovereignty).

³⁰ 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); Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM/2022/68 final.

The claims of the EU as a political and economic union, and of EU Member States individually, both revolve around a geographical version of sovereignty in that they seek the power to regulate and to achieve strategic autonomy in the digital environment.³¹ These claims, on the one hand, aim to safeguard the EU's economic self-determination and digital transformation on the basis of European values.³² Various EU Member States support for example the European Gaia-X initiative, which aims to establish a federated native European data infrastructure that would ensure “data sovereignty by design”, in order to create an alternative to closed digital ecosystems provided by dominant foreign corporations.³³ The EU also exports its rules beyond the confines of EU territory to govern foreign companies that supply services to the EU single market or to regulate cross-border data flows.³⁴ An example of the latter digital sovereignty claims is the regulation of the cross-border collection of personal data and their transfer to third countries pursuant to the General Data Protection Regulation.³⁵

Digital sovereignty claims by local governments

Digital sovereignty claims are by no means limited to the higher levels of government; on the contrary, local governments also assert digital sovereignty and devise actions to act on these claims. In the specific context of “smart cities”, digital sovereignty claims arise as part of a broader agenda to reimagine and remake smart cities as places of democratic, emancipatory, inclusive and sustainable urban governance, with municipalities warning against platform urbanism and techno-capitalistic digitalisation of cities.³⁶ Local governments' awareness of the transformational power of strategic public procurement is increasing (see below).

Smart cities

According to ‘Smart City Dialog’ – a German collaborative platform established in 2016 to “shape the digital transformation in the municipalities in a sustainable way”³⁷ – data sovereignty is “a key issue for municipalities when it comes to their democratic self-determination as smart cities.”³⁸ It argues that municipal administrations “need to have access to data required to perform their tasks and develop innovative services to ensure their digital sovereignty”.³⁹ In order to safeguard such data access, the city of Barcelona pioneered the inclusion of special ‘data sovereignty clauses’ in its public procurement contracts, requiring its suppliers to share back the data they gather in the course of delivering services to the city in machine-readable format.⁴⁰

Digital sovereignty claims by private sector organisations

A lack of control over data and/or dependencies on foreign providers of digital technologies and infrastructure has also led a variety of private sector organisations such as businesses, business groups and cooperatives to claim digital sovereignty. Claims related to dependencies on foreign providers are often addressed to governments, involving requests to create more European capacities, to strengthen businesses' legal positions vis-à-vis powerful technology companies and to reduce dependencies in certain strategic sectors such as information security. Such claims are likely to benefit both the national economy and security, as well as the organisations operating in that economy. Claims related to data sovereignty, on the

³¹ Christakis 2020, p. 5-6, Timmers 2019, p. 641; Moerel and Timmers 2020, p. 5, 7, 25.

³² Christakis 2020, p. 11; Pohle and Thiel 2020, p. 8.

³³ See Franco-German Position on Gaia-X 2020, p. 10.

³⁴ Christakis 2020, p. 11; Pohle and Thiel 2020, p. 8.

³⁵ Irion 2022.

³⁶ Morozov and Bria 2018; Kitchin 2018; Vadiati 2022.

³⁷ Smart City Dialog, ‘Dialogue Platform’, <<https://www.smart-city-dialog.de/en/dialogue-platform>>.

³⁸ Smart City Dialog, ‘Data Sovereignty: a key issue for municipalities’, <<https://www.smart-city-dialog.de/en/news/data-sovereignty-a-key-issue-for-municipalities-2>>.

³⁹ German Federal Institute for Research on Building, Urban Affairs and Spatial Development 2021, p. 19.

⁴⁰ Bria 2020. It should be noted, however, that such claims for data access are typically not only based on arguments of data sovereignty but also on the utility of the data for e.g., law enforcement and public order purposes.

other hand, typically concern the access to and availability of data and distribution of value extracted from these data.

A survey among German companies

A 2021 survey among 1219 German companies in the information technology and manufacturing sectors shows that more than half of the companies in both sectors view digital sovereignty of high or very high importance for the long-term success of the company, and even more so for the entire German economy.⁴¹ Digital sovereignty claims by organisations focus primarily on data sovereignty aspects, interoperability and modularity of IT systems (lock-ins and switching costs), and dependencies on non-European providers of software, applications and hardware.⁴² More than two-thirds of the companies indicated that their dependence on non-European suppliers was caused by a lack of equivalent EU-alternatives.⁴³

DSN and DECODE

The Data Sovereignty Now (DSN) initiative, ran by a coalition of private stakeholders (thinktanks, research organisations, data management service providers, etc.), aims to contribute to policy debates at EU and Member States' levels on data sharing in order to counter big tech monopolies on the exploitation of data.⁴⁴ DSN highlights the systemic problem that individuals and organisations who generate data do often not get a fair share of benefits from its exploitation,⁴⁵ since these benefits are concentrated in the hands of a few tech companies. DSN therefore pitches “data sovereignty” as a solution to “realign the ‘data benefit balance’”.⁴⁶ Furthermore, the DECODE project, led by a consortium of 15 partners from across Europe, approaches data as a common infrastructure and develops decentralised digital applications to allow communities to leverage the value of their data collectively and to enable their digital rights. These applications include, for instance, a smart contracts engine, an authentication app and an interactive dashboard to share urban data.⁴⁷

Digital sovereignty claims by or to the benefit of individuals

Finally, digital sovereignty claims made by individuals are rooted in ideals of user autonomy and self-determination of individuals in different societal roles – as citizens, employees, consumers and users of digital technologies and services.⁴⁸ Addressees of these claims can be governments (e.g., in the context of the government use of digital technologies capable of undermining fundamental rights) and organisations (e.g., in consumer protection or the employment context). Individuals' digital sovereignty claims are rarely effective on their own and are often made by policymakers, civil society actors and more recently, various types of data intermediaries (such as data trusts) in the interest of individuals. Personal data protection and consumer protection can be mentioned as examples of individuals' digital sovereignty claims.⁴⁹

On-demand app drivers

On-demand app delivery workers, such as private hire drivers using apps like Uber and Ola, are often subject to large-scale data processing and algorithmic management, including facial recognition and automated deactivation. In recent years, the number of court cases filed by individual platform workers, trade unions (e.g., UK App Drivers & Couriers Union) and civil society organisations (e.g., Worker Info Exchange) on data

⁴¹ Seifried et al 2021, p. 44.

⁴² Ibid., p. 40-57.

⁴³ Ibid., p. 49.

⁴⁴ See the website of Data Sovereignty Now (DSN), <<https://datasovereignty.org/our-mission/>>.

⁴⁵ DSN Position Paper 2021.

⁴⁶ Ibid.

⁴⁷ DECODE, 'DECODE gives back Data Sovereignty to Citizens', <<https://tools.decodeproject.eu/>>.

⁴⁸ The notion of consumer sovereignty is an economic concept coined by William Harold Hutt, grounded in the social ideal of liberty and viewed as a means of promoting political and social stability. See e.g., Desmarais-Tremblay 2020, p. 15; Persky 1993; Pohle and Thiel 2020, p. 11-12.

⁴⁹ Ibid., p. 12.

protection infringements has been on the rise in an attempt to demand transparency and control over workers' personal data.⁵⁰

1.2.3 Meaning of digital sovereignty

Now that it is clear who can claim digital sovereignty (governments, private sector organisations and individuals) and what the objects of these claims can be (sovereignty in relation to digital technologies/infrastructures and data), the next question is: what does it exactly mean to “have” sovereignty over digital infrastructures and data? In literature, numerous terms have been used to define and describe the concept of digital sovereignty, including ‘control’, ‘self-determination’, ‘independence’, ‘strategic autonomy’ and ‘the ability to make one’s own choices’.⁵¹ Some scholars argue that digital sovereignty is not just about being able to control technological infrastructures by applying one’s own policies to them, but also – or fundamentally – about being sufficiently knowledgeable and capable to (re)build and maintain infrastructures by oneself, independently from other parties.⁵² In other words: if you cannot build and operate your own digital systems, you are not actually digitally sovereign. This indeed holds true when it comes to *foundational research* into digital technologies, such as Artificial Intelligence.⁵³ For all other cases, however, this report – while not dismissing the value of self-hosted digital infrastructure – does not rule out that a sufficiently high level of digital sovereignty can be achieved even while using technologies and infrastructures built and maintained by third (commercial) parties. It thus takes the view that digital sovereignty does not imply autarchy.⁵⁴ Without trying to exhaustively define the concept, this report argues that universities’ digital sovereignty claims as discussed in Chapter 3 share a common need for self-determination in the digital space⁵⁵ and for the ability to take autonomous decisions and actions regarding digital infrastructures as well as the data residing in those infrastructures (i.e., decisions on the design of, access to and use of systems and on the affordances of data).⁵⁶

1.3 Digital sovereignty in the university sector

The digital sovereignty discourse has moreover reached the university sector.⁵⁷ The digital transformation of academic research and teaching activities, and of universities’ operations more generally, has raised concerns similar to those expressed by other economic sectors about diminishing control over digital technologies, infrastructures and the (research) data stored in and generated by these technologies and infrastructures. Public value-oriented universities fear the erosion of academic values and institutional autonomy which, ultimately, could affect their ability to contribute to scientific advancement. The following subsections briefly explore how universities have digitally transformed and, simultaneously, have become more dependent on commercial digital technology providers. Section 1.4 concludes the Chapter by introducing a model of digital sovereignty claims for the university sector that will guide the remainder of this report.

⁵⁰ See Ausloos, Toh and Giannopoulou 2022; see also Amsterdam Court of Appeal 4 April 2023, ECLI:NL:GHAMS:2023:804; Amsterdam Court, 11 March 2021, ECLI:NL:RBAMS:2021:1020.

⁵¹ See e.g., Pohle 2020; Pohle and Thiel 2020; Moerel and Timmers 2020; Stolwijk et al 2022; Madiaga (European Parliamentary Research Service) 2020; German Federal Ministry for Economic Affairs and Energy 2019.

⁵² Fiebig and Aschenbrenner 2022, p. 4.

⁵³ For example, when conducting research into Artificial Intelligence (AI), researchers must be able to create an AI-system by themselves and not only build on top what is being provided by third parties.

⁵⁴ See also Pohle 2020, p. 8.

⁵⁵ Pohle 2020, p. 8; Pohle and Thiel 2020, p. 8.

⁵⁶ Moerel and Timmers 2020, p. 6.

⁵⁷ See e.g., Schultz et al 2022; Jansen 2021.

1.3.1 Digitalisation and datafication of universities

Just as many other organisations in the private and public sectors, universities’ core functions nowadays are mediated by a wide variety of digital tools and infrastructures. Some of these tools are centrally procured as part of universities’ digital portfolios (e.g., electronic learning environments such as Canvas, Blackboard, plagiarism tools such as Turnitin, productivity tools such as Microsoft Office and research information management systems such as Pure), while others are used – often for free – of academics’ own accord (e.g., Google Scholar, Academia). A non-exhaustive overview of digital tools commonly used by and within Dutch universities is provided in Table 1.⁵⁸ In parallel, the production and use of digital data within universities has increased exponentially, not only in the context of academic research but also as input for institutional decision-making processes (e.g., productivity data relating to staff-, student- and institutional performance).⁵⁹

| | Digital tools | | |
|-----------------------|--|---|---|
| Research | <u>Before the research:</u> <ul style="list-style-type: none"> ▫ Software for the creation of data management plans (e.g., DMP online) ▫ Software for research management (e.g., Research Management Services - RMS) | <u>During the research:</u> <ul style="list-style-type: none"> ▫ Experimental systems (e.g., Internet of Things test labs) ▫ High performance computing capabilities (e.g., LISA Rekencluster) ▫ Academic search engines (e.g., Google Scholar) ▫ Online academic libraries (e.g., JSTOR, Wiley Online Library, SSRN) ▫ Bibliometric platforms (e.g., Scopus, Google Scholar) ▫ Data storage platforms (e.g., SURF Research Drive, OneDrive) ▫ Data analysis software (e.g., Qualtrics, Stata, Python) ▫ Application software (e.g., MS 365, including Teams) | <u>After the research (scientific communication):</u> <ul style="list-style-type: none"> ▫ Research data repositories (e.g., UvA/HvA figshare) ▫ Research output databases (e.g., UvA DARE, Pure) ▫ Current Research Information Systems (e.g., Pure) ▫ Data sharing tools (e.g., Amsterdam Research Data Exchange – AMDEX) |
| Education | <ul style="list-style-type: none"> ▫ Student information systems (e.g., OSIRIS) ▫ Learning management systems (e.g., Moodle (self-hosted), Blackboard (hosted by Microsoft Azure), Courseleaf (located in Amazon EC2)) ▫ Remote teaching software such as video chat tools and streaming solutions (e.g., Zoom, Microsoft Teams, WebEx, BigBlueButton (self-hosted)) ▫ Examination and proctoring software (e.g., TestVision, Proctorio) ▫ Plagiarism detection tools (e.g., Turnitin) ▫ Multi-media systems (e.g., Kaltura) | | |
| Administration | <ul style="list-style-type: none"> ▫ Budgeting and accounting tools ▫ HR systems, including personnel management databases and applicant management databases ▫ Foundational services (e-mail, university network, Teams) ▫ Student admission services ▫ Security management services ▫ Research productivity and performance tools | | |

⁵⁸ Mainly based on an internal overview of central ICT infrastructure for research used by the University of Amsterdam and Fiebig e.a. 2023, p. 2.

⁵⁹ See e.g., Williamson 2021, p. 61-62; Williamson, Bayne and Shay 2020; Goldenfein and Griffin 2022.

Table 1. Examples of digital applications used by Dutch universities

1.3.2 Commercialisation of the digital academic sphere

Traditionally, universities were viewed as “pioneers in deploying and maintaining their own digital infrastructure”.⁶⁰ Over the past decades, however, they have been outsourcing the development and management of formerly self-hosted digital infrastructures and services to commercial, often non-European suppliers, while unceasingly adding new digital services to support research and education. By and by, universities have become reliant on commercial suppliers of digital infrastructures, software and tools who anticipated the growing needs of the university sector and jumped into the market to enable the sector’s digital transformation. In other words, universities’ digital structures have been “commercialised”.⁶¹

The shift from self-hosting to outsourcing and procurement could be explained by the rise of global technology companies with tremendous digital expertise and resources offering high-quality and seamlessly connected infrastructures at lower costs.⁶² First, outsourcing supposedly reduces the direct monetary costs of digital infrastructures because cloud computing typically has the benefit of scale and does not require investments in local staff and expertise to maintain them.⁶³ A counterargument, however, is that universities must also take into account the potential migration costs incurred in the event of switching between providers, but that aside.⁶⁴ Second, outsourcing seems to be strongly associated with product quality and convenience. University representatives have indicated that many digital infrastructures used in academia do not have viable public equivalents that possess the same level of functionality and user-friendliness as those offered by the private sector (see examples below).⁶⁵ While the outsourcing process was already ongoing, it was significantly boosted in 2020 by the outbreak of the COVID-19 pandemic, as a result of which universities were forced to quickly adopt even more digital solutions (especially videoconferencing tools⁶⁶) to ensure the continuity of their teaching and research activities,⁶⁷ and commercial suppliers were pressured to accelerate the rollout of existing EdTech projects.

Examples of commercial outsourcing in the Dutch higher education sector

A pilot initiated by SURF⁶⁸ in March 2020 into the use of ‘Jitsi’ – an open source video-conferencing tool to be installed on local instances – was terminated after nine months because the Dutch universities indicated they had already been “satisfied” with the commercial video-conferencing tools available on the market.⁶⁹ Eindhoven University of Technology (TU/e) decided in 2019 to switch to Microsoft Office 365, arguing that Office 365 would, amongst other things, “offer better opportunities for collaboration” and “better data security in the future”.⁷⁰ Nyenrode Business University justified its decision to introduce a unified IT infrastructure (Microsoft Azure Unified Pipeline) by stating that its old IT environment was a scattered whole of individual applications that had to work together – “a complicated spaghetti dish with melted cheese all over it” – and that it wanted to transform this environment into an “integrated whole”.⁷¹

⁶⁰ Angeli et al 2022, abstract and p. 3. In 2001, for example, Utrecht University introduced its self-developed student information system ‘OSIRIS’, facilitated until 2012 by the Amsterdam-based company ‘PSB Informaticsystemen’, see Belleman and Van Dijk 2022 and Sanders 2012.

⁶¹ Hogan 2018; Williamson 2021, p. 52-53.

⁶² Angeli et al 2022, p. 1, 3. See also Fiebig et al 2023, p. 2: “...universities look towards cloud infrastructure as a way to reduce their own IT investments...”

⁶³ Angeli et al 2022, p. 3; Fiebig et al 2023, p. 2; Mayer-Schönberger 2020, p. 123-125.

⁶⁴ Fiebig et al 2023.

⁶⁵ KNAW 2022, p. 49; also argued by representatives of Dutch universities and universities of applied sciences at the “SURF Summit 2022” on Digital Sovereignty, an event organised by the Dutch IT organisation for higher education and research SURF.

⁶⁶ Hence the term “zoomification” of higher education, see Fiebig et al 2023, p. 8.

⁶⁷ Amankwah-Amoah et al 2021; Williamson and Hogan 2021.

⁶⁸ The collaborative organisation for IT in Dutch education and research, see <<https://www.surf.nl/en>>.

⁶⁹ Van Santen (SURF), ‘UPDATE: Videobellen: snel, simpel en veilig’, 9 May 2022, <<https://communities.surf.nl/artikel/update-videobellen-snel-simpel-en-veilig>>.

⁷⁰ Van Gaal 2019.

⁷¹ Microsoft Customer Stories 2021.

It should be noted that not all university infrastructures and digital tools are provided by the market. Self-hosted alternatives still exist and are typically developed and provided in the context of multi-university partnerships.⁷² The degree and manner of digital outsourcing also seems to vary per country and region according to socio-economic factors, including a different historical understanding of what higher education means and a different valuation of academic independence.⁷³ At Dutch universities, for example, the percentage of externally hosted applications increased rapidly from 39% in 2016 to 87% in 2020.⁷⁴ While Dutch, British and also American universities are keen users of commercial cloud-based services, the uptake of these services by universities in for example France, Germany and Austria has been significantly lower with less than 50% of universities relying on cloud providers for any services in 2023.⁷⁵

Against the trend: examples of ICT self-hosting

The German university of Osnabrück is an exception to the outsourcing trend in that it maintains its own data centre and software and instead of commercial videoconference services uses the open source program BigBlueButton.⁷⁶ During the COVID-19 pandemic, the Delft University of Technology also introduced BigBlueButton as an alternative for Zoom, a pilot project which has however been discontinued as of June 2023.⁷⁷ Another exception to the rule is GÉANT, a European collaborative organisation of national research and education networks (NRENs), which has developed multiple digital services to support researchers and educators (e.g., identity verification services, VPN services, firewall-on-demand services, etc.).⁷⁸ GÉANT also funds the coordination of the infrastructure underlying the global service “eduroam”, a service which enables the international research and education community to obtain Internet connectivity on the campuses of participating institutions.⁷⁹

From Twitter to Mastodon

In February 2023, the Dutch collaborative organisation for IT in research and education ‘SURF’ created a server within the increasingly popular non-profit platform ‘Mastodon’, specifically aimed at universities in the Netherlands, to facilitate discussions on science and higher education and reduce universities’ dependency on Twitter.⁸⁰

Overall, the ICT-outsourcing by both public and private organisations has been a global trend from which commercial digital technology providers greatly benefit, not only financially but also in terms of influence. The literature proposes a number of theories that explain how suppliers of digital technologies and infrastructure could wield influence over other organizations and in particular universities: (1) sphere transgression, (2) platformisation and (3) digital colonisation.

(Digital) sphere transgression

⁷² In the Netherlands, for example, the collaborative organisation for IT in research and education ‘SURF’ has developed multiple non-commercial services such as cloud storage (SURFdrive, Research Drive), a file sending application (SURFfilesender) and a portal for the creation of virtual research workspaces (SURF Research Cloud). A non-exhaustive overview of other open, non-commercial infrastructures for higher education and research, put together by (former) librarians of Utrecht University, can be found here: <<https://tinyurl.com/open-infrastructure>>.

⁷³ Fiebig et al 2023.

⁷⁴ Bok et al 2021 (VSNU), p. 29.

⁷⁵ Fiebig et al 2023, p.5.

⁷⁶ Vleugels and Van Wijnen 2022 (*Het Financieele Dagblad*).

⁷⁷ See <<https://bbb.tbm.tudelft.nl/b>> (last visited 16 May 2023).

⁷⁸ See <<https://geant.org/services/>>.

⁷⁹ See <<https://eduroam.org/about/>>.

⁸⁰ See <<https://www.surf.nl/over-de-mastodon-pilot>> and <<https://medewerker.uva.nl/bestuursstaf-gde/shared-content-secured/medewerkersites/uva-medewerkers/nl/nieuws/2023/03/uva-doet-mee-aan-mastodon-pilot-ijj-ook.html?cb>>.

The theory of “sphere transgression”⁸¹ aims to explain the phenomenon where commercial technology providers are converting their technical and digital expertise – in respect of infrastructure development, data collection and data analytics – into advantages in other societal-economic sectors, or ‘spheres’, such as health, news provision, mobility, finance, politics, security, and indeed, education and science. The theory builds on the work of the political philosopher Michael Walzer, who argued that in a just society, advantages gained in one sphere should not lead to advantages in other spheres. For example, wealth in the market sector should not lead to power in the political sector.⁸² The digitalisation of the 21st century, however, has set in motion a profound transformation of society whereby ICT “is no longer a specific sector” but by transgressing other sectors’ boundaries has become “the foundation of all modern innovative economic systems and societies.”⁸³ While this could be regarded as a positive development leading to technical efficiency and other benefits in various sectors, it also comes with serious risks. Risks identified in sphere transgression-literature are, for example, the ‘crowding out’ of traditional sectorial practices, norms and values and the reshaping of spheres according to commercial-technical values and interests; the emergence of new dependencies on private commercial actors for the delivery of essential public goods; the shaping of public policies by non-representative and non-accountable technology companies; and ultimately, the accumulation of advantages and power across multiple spheres leading to ‘tyranny’.⁸⁴ The particular consequences of the growing presence of commercial technology providers in the university sector are discussed in Chapter 3 of this report.

Platformisation

Complementing the theory of sphere transgression, which looks at the growing influence of technology companies *more broadly*, the theory of ‘platformisation’ specifically focuses on the mounting power *of digital platforms*.⁸⁵ Platforms can be defined as programmable and data-driven digital infrastructures that facilitate and shape personalised interactions between product or service providers and end-users.⁸⁶ Examples of platforms are social media (Facebook, Instagram, Twitter) but also – relevant to the university sector – Microsoft’s Office suite, and research-focused systems such as Google Scholar, ResearchGate and Academia.edu. Platformisation, then, can be understood as “the penetration of the infrastructures, economic processes, and governmental frameworks [by] platforms in different economic sectors and spheres of life”.⁸⁷ In literature, the platformisation of higher education has been critically discussed for redefining the (higher) education sector by inflecting or disrupting democratic public values with techno-commercial architectures of corporate platforms.⁸⁸

Digital colonisation

Lastly, the theory of ‘digital colonisation’ explicitly discerns a pattern of *deliberate* penetration by commercial digital technology providers, including platforms, of the higher education sector, namely with the aim of capturing data and leveraging data analysis capabilities to produce data-driven insights (i.e., adding value) to be sold to educational institutions and/or inform the design and commercialisation of new products and

⁸¹ Or “sector creep”, see Sharon 2020, referring to Walzer 1983; see also Tamar Sharon at the PublicSpaces Conference 2022 (video), <<https://conference.publicspaces.net/en/session/keynote-bu>>. See also the online Sphere Transgression Watch digital tool which visualises sphere transgression over time: <<https://www.sphere-transgression-watch.org/>>.

⁸² Walzer 1983.

⁸³ Recital 1 of Regulation (EU) 2018/1807 of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union.

⁸⁴ Sharon 2020, p. 551-554.

⁸⁵ Poell, Nieborg and Van Dijck 2019.

⁸⁶ Based on Poell, Nieborg and Van Dijck 2019, p. 3.

⁸⁷ Poell, Nieborg and Van Dijck 2019, p. 5-6.

⁸⁸ Van Dijck, Poell and De Waal 2018, p. 117-136; Nicholds and Garcia 2022.

services for the sector.⁸⁹ When procuring services and contracting with commercial suppliers, universities do often not realise or preclude that the companies' business models are built on the collection and exploitation of data.⁹⁰ The substantial amounts of data⁹¹ processed within educational institutions' digital infrastructures render the infrastructures valuable resources for data analysis, which can yield data-driven insights to infuse commercial product improvement and development processes.⁹² Moreover, aggregated data can be repackaged into metrics which, in turn, can be advertised to universities to enhance their institutional decision-making processes. In this scenario, universities' self-generated data are basically sold back to them.⁹³ The strategy of leveraging the supply of digital infrastructures in order to capture value from data and of then selling new (analytics) services or products back to universities could be considered extractive, as it deprives academic institutions from value that they mainly generate themselves, usually with public money.⁹⁴ Digital technology providers deliberately 'infiltrate' into the sector to become "unique providers of critical, data-driven value",⁹⁵ thereby changing power dynamics and "commoditizing"⁹⁶ the parties using their services.

In sum, all theories warn of the risks of the commercialisation of the digital public sphere, and/or the digital dimension of higher education specifically. These risks essentially boil down to the overarching concern that commercial digital technology providers 'infiltrate' in public-interest driven sectors and erode (or: crowd-out, reshape) public values – including academic values – anchored in these sectors. It is therefore of utmost importance that the digital transformation of universities is closely monitored to ensure that it conforms with public values. To that end, the next section proposes a model to assess the digital sovereignty of universities.

1.4 A model for digital sovereignty in the university context

As will be discussed in more detail in Chapter 3, the commercialisation of the digital academic sphere has sparked several issues revealing universities' and academics' diminishing control over digital infrastructures and data. These issues have given rise to corresponding "claims" for digital sovereignty that serve to restore, protect and promote normative values central to academia. To be specific, universities' and academics' digital sovereignty *claims* arise from, and are defined by, certain *issues* or *threats* that have developed from the commercialisation of the digital space and that affect *academic values* (Image 2). For public value-oriented universities that claim digital sovereignty, this model can be used to formulate appropriate responses to different types of claims, and ultimately, to defend the values that lie at the heart of the university sector.

⁸⁹ Ozalp et al 2022, p. 83-84.

⁹⁰ Maex et al 2019.

⁹¹ That is, both "existing" data held by universities and uploaded to the systems, and "user-generated" (meta)data following from users' behaviour while using the infrastructures. See Ozalp et al 2022 about the data capture strategies of Google, Amazon, Facebook, Apple and Microsoft; see also DFG Briefing Paper 2021 and Aspesi et al 2019a (SPARC Landscape Analysis) about data capture by academic publishers.

⁹² Ozalp et al 2022; Sellar and Hogan 2019, p. 4, 10, 11; Williamson and Hogan 2020, p. 62; see also Mayer-Schönberger 2020, p. 129 on "feedback data".

⁹³ SPARC 2022 (Interfolio Acquisition Report).

⁹⁴ Mainly, because the economic value lies in the *aggregated* data and the aggregation is carried out by the commercial provider and not by universities.

⁹⁵ Ozalp 2022, p. 84. In the remainder of this report, however, we prefer to use the more neutral phrase "expansion of influence" rather than "colonization".

⁹⁶ Ibid.

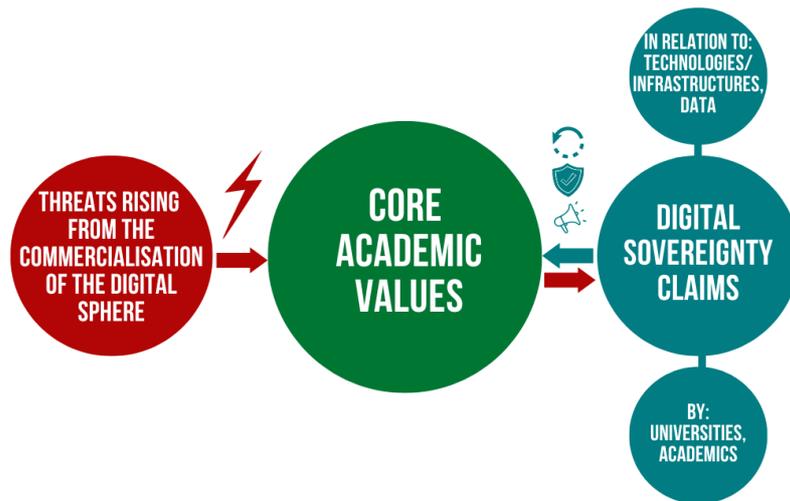


Image 2. A model of digital sovereignty for the university context

It has become apparent from this Chapter that digital sovereignty claims are not limited to states or state-like unions but can also be made by other actors such as private sector organisations and individuals. Against this backdrop, it is concluded that both academic institutions and academics (individually or collectively) are able to make claims in the interest of their digital sovereignty.

It should be emphasised that the digital transformation of society and the commercial outsourcing of ICT *as such* are not considered the primary causes for universities' and academics' claims for digital sovereignty. Rather, the claims arise from the ongoing capture of internal processes, operations and data by a handful of large digital technology providers, putting universities' self-governance and the realisation of academic and public values at risk. Various theories proposed in literature (e.g., sphere transgression, platformisation and digital colonization) warn about the risk of important public values eventually being eroded or replaced by the techno-commercial logic of commercial providers.

As a critical reflection, it could be argued that digital sovereignty as a concept is not particularly necessary to assess the threats that universities face in connection with the commercialisation of the digital academic sphere. In fact, the term adds an extra interpretational layer to an already complex discussion on the future of universities as autonomous knowledge institutions. Digital sovereignty is also not an issue unique to the university sector *per se*; it has been used by numerous other societal actors to describe digital autonomy concerns. Fundamental academic values, by contrast, *are* unique (see Chapter 2) and require universities to charter a careful course through the digital transformation. There may therefore be something to say for putting these values at the forefront of the discussion, using terminology more tailored to universities. At the same time, however, the benefit of the digital sovereignty-concept is that it directly speaks to the digital aspect of broader autonomy concerns, giving these specific concerns a 'label', so to say, and making them more tangible. This, together with the fact that it links to a broader discourse, makes 'digital sovereignty claims' a good shorthand to describe a set of complex threats to academic values.

2. Normative underpinnings of digital sovereignty claims in the university context

As demonstrated in Chapter 1, digital sovereignty must not be seen as an end in itself, but rather as a means to restore, protect and promote higher normative values in the ongoing digital transformation. In the university context, three values in particular require such protection: (1) **scientific advancement**, (2) **individual academic freedom** and (3) **institutional autonomy**. These values have been the rationale for founding public universities, and more importantly, guide universities' commitments and activities in the fulfilment of their public-interest mission (section 2.1). Based on a review of legal and declaratory documents, this Chapter traces the meaning of the aforementioned academic values in order to gain a better understanding of the normative underpinnings of universities' claims for digital sovereignty, i.e., of why digital sovereignty must be attained (sections 2.2 – 2.3). Due to the limits of the report, the Chapter only focuses on values that lie at the very heart of academia, including those intricately linked to this core such as openness and transparency, privacy and data protection, and economic autonomy. Other relevant values that underlie university culture such as accountability, integrity, equality and inclusivity, equitable access, social connection and collegiality, collaboration etcetera, are recognised as important building blocks of the university sector but will not be specifically addressed in this report.⁹⁷

2.1 Universities' role in society

Since their establishment, universities have taken on the role of “keepers of a culture of knowledge” and “agents of new knowledge”.⁹⁸ This is not to say, of course, that knowledge production is exclusively reserved for universities. Government research agencies,⁹⁹ independent research institutes and hospitals,¹⁰⁰ amongst others, also conduct meaningful scientific research, and the role of the private sector should not be underestimated either. Collaborations between academics and commercial partners – e.g., through

⁹⁷ For an overview of those values, see Scholars at Risk 2020; SURF and Kennisnet 2021 (“Value Compass”); Science Europe 2022.

⁹⁸ Maex and Bakker 2022, p. 39; UNESCO 1997, para. III.4: “The pursuit of new knowledge and its application lie at the heart of the mandate of such institutions of higher education”. See also Ayris, in: LERU New Year’s Debate 2022 (00:08:05 and further) and the LERU Data Statement 2021, p. 1.

⁹⁹ E.g., the Defense Advanced Research Projects Agency of the US Department of Defense (DARPA) and the Research and Documentation Centre of the Dutch Ministry of Justice and Security (WODC).

¹⁰⁰ Recital 12 of Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market.

sponsorships or the sharing of equipment¹⁰¹ – are widespread. Plus, large corporations often run their own research and development departments.¹⁰² However, despite the growing contribution of commercial actors to scientific research, research-intensive universities and academics are still considered the vanguard of contemporary science, not in the least because public value-oriented universities are uniquely positioned for the production and distribution of knowledge.

There are several features setting universities apart from other organisational actors. First, universities are typically durable and therefore reliable institutions. Some of them have been around for almost a millennium,¹⁰³ thus providing a consistent forum for academics and students to research, teach and learn. For-profit entities, on the other hand, tend to emerge, change course and exit depending on business decisions and economic prosperity. For instance, if Alphabet Inc. would decide that the costs of keeping Google Books are too high and therefore discontinue the service, it remains to be seen whether all the scanned books, i.e., collective knowledge, saved on their private infrastructures would continue to be available.¹⁰⁴

Secondly, universities traditionally have a public function to serve society as a whole.¹⁰⁵ Based on their social contract with the public, universities bear responsibilities; to fulfil these they have necessary privileges (academic freedom and institutional autonomy, see section 2.2).¹⁰⁶ Universities are mandated to develop, extend and advance universal knowledge for the benefit of humankind;¹⁰⁷ respond to contemporary problems of public concern;¹⁰⁸ contribute to human development, social, economic, technical and cultural advance;¹⁰⁹ encourage the development and maintenance of democratic culture, social order and a sense of basic values in societies;¹¹⁰ promote principles of freedom, justice, human dignity and solidarity;¹¹¹ invest in the education and training of future generations;¹¹² share information with the international community;¹¹³ and contribute to a prosperous and sustainable future.¹¹⁴ Simply put, universities are thought of as the “guardian[s] of scientific knowledge”, embedded in and engaged with the world,¹¹⁵ expected to serve the common good according to public values.¹¹⁶ For-profit entities, on the other hand, do not bear such societal responsibilities, which means that they will prioritise economic self-interests over the public interest where necessary (see example below).

Thirdly, academic research is in principle characterised by national and international collaboration and verification processes such as independent peer review, dialogue and critique.¹¹⁷ These longstanding

¹⁰¹ European Data Protection Supervisor (EDPS) 2020, p. 7-8. For example, sponsored clinical research and support in the form of investigational compounds in the pharmaceutical industry.

¹⁰² E.g., Google Research, <<https://research.google/>>.and Amazon science, <<https://www.amazon.science/tag/research-development>>.

¹⁰³ The University of Bologna was founded in 1088 and is considered as the oldest university of the Western world, see <<https://www.unibo.it/en/university/who-we-are/our-history/our-history>>.

¹⁰⁴ Vaidhyathan 2011, p. 165; Newton 2013.

¹⁰⁵ Magna Charta Universitatum 1988, Preamble under 1-2.

¹⁰⁶ Parliamentary Assembly of the Council of Europe, Recommendation 1762 (2006), para. 6.

¹⁰⁷ Parliamentary Assembly of the Council of Europe, Recommendation 1762 (2006), para. 5; Committee of Ministers of the Council of Europe, Recommendation CM/Rec(2012)7, Preamble, p. 2; Committee of Ministers of the Council of Europe, Recommendation No. R (2000) 8, Preamble; Magna Charta Universitatum 1988, Preamble para. 1; International Association of Universities (IAU) 1998, Preamble; American Association of University Professors (AAUP) 1915, p. 4.

¹⁰⁸ Committee of Ministers of the Council of Europe, Recommendation No. R (2000) 8, para. 1.1; see also International Association of Universities (IAU) 1998.

¹⁰⁹ International Association of Universities (IAU) 1998, p. 1.

¹¹⁰ Committee of Ministers of the Council of Europe, Recommendation CM/Rec(2012)7, Preamble, p. 2; Parliamentary Assembly of the Council of Europe, Recommendation 1762 (2006), para. 9.

¹¹¹ Preamble of the Constitution of the International Association of Universities (IAU) 2019.

¹¹² Magna Charta Universitatum 1988, Preamble, Principle 2.

¹¹³ In particular with developing countries, communities living in poverty and groups with special needs and vulnerabilities, see Article 15 of the International Covenant on Economic, Social and Cultural Rights (ICESCR) jo. Committee on Economic, Social and Cultural Rights (CESCR), para. 80. See also Sorbonne declaration 2020.

¹¹⁴ Joint Statement by ALLEA, EUA and Science Europe 2019, p. 1.

¹¹⁵ Steele and Rickards 2021, p. 70-71.

¹¹⁶ Maex 2021, p. 4.

¹¹⁷ Although so-called ‘predatory journals’ do exist, that is, journals that do not provide for (decent) peer review or other quality checks, see e.g., <<https://www.nature.com/articles/d41586-019-03759-y>>.

practices, self-developed by various scientific communities, aim to safeguard the integrity of research and improve the quality of scientific papers. Such control mechanisms may not always be in place (yet) in government or corporate research facilities. All things considered, universities and academic researchers are arguably the most appropriate agents to drive scientific progress.

Indeed, driving progress by means of science is what universities have been doing for decades, using their privileges to create tangible benefits for society. Researchers affiliated with universities have made outstanding contributions to science;¹¹⁸ teachers at universities have trained generations of leaders, innovators and skilled citizens; and businesses have grown due to knowledge exchanges in university-industry partnerships. Considering the large research grants which European universities receive every year from both governmental and non-governmental actors, it seems that their contributions are still highly appreciated by the general public.¹¹⁹

Charging for open access

The commercial scientific publishing industry illustrates how dependencies on economically self-interested parties may complicate the dissemination of knowledge in the public interest. For a long time, the dominant business model of commercial scientific publishers had been to capture academic research behind paywalls and to make interested parties, in large part (public) universities, pay journal subscription fees to access the content. As a result, publicly funded universities have been paying for the work produced by their very own researchers. Current trends in open science have pushed many publishers towards open access publishing and hybrid models. But these models, too, come with a price tag. Academic institutions are typically charged high fees to compensate publishers' efforts to organise peer review and to publish, archive and index open access articles.¹²⁰ Open access publishing has become a business model as well,¹²¹ benefiting publishers' generally substantial profit margins..

2.2 Academic values and their legal articulation

Scientific advancement can be considered as the “mother” of academic values; all other academic values aim to contribute to that objective. Arguably, the most important value underpinning scientific advancement is academic freedom. Academic freedom, in turn, has both an individual and institutional dimension. The two components are referred to in this report as ‘individual academic freedom’ and ‘institutional autonomy’, respectively.¹²² The relationship between the core academic values – scientific advancement, individual academic freedom and institutional autonomy – is visualised in Image 3 below. On the basis of international and European human rights law, soft law instruments and declarations drafted by the academic community and civil society, this section will clarify the meaning of these three core values, and where relevant, touch upon related concepts. This value-mapping exercise will help to acquire a better understanding of universities’ different types of digital sovereignty claims (Chapter 3).

¹¹⁸ For example, 121 affiliates of the University of Cambridge have been awarded the Nobel Prize since 1904, which are more than any other institution, see <<https://www.cam.ac.uk/research/research-at-cambridge/nobel-prize>>.

¹¹⁹ For example, the budget of the European Research Council for 2021-2027 is over €16 billion, see <<https://erc.europa.eu/about-erc/erc-glance>>.

¹²⁰ Article Processing Charges, or APCs, see e.g., <<https://www.springeropen.com/get-published/article-processing-charges>>. Moreover, “double dipping” – i.e., collecting both APCs and non-reduced subscription fees via so-called hybrid journals which contain both open access and subscription articles – may occur. See Prosser 2015, <<https://www.rluk.ac.uk/the-costs-of-double-dipping/>>.

¹²¹ See also The Guild 17 May 2022.

¹²² Individual academic freedom and institutional autonomy are considered as “the basic and inalienable conditions” that enable universities and academics to fulfil their responsibilities towards scientific advancement, see International Association of Universities (IAU) 1998; see also Committee on Economic, Social and Cultural Rights (CESCR) General Comment No. 13 1999, para. 38-40; Committee of Ministers of the Council of Europe Recommendation CM/Rec(2012)7, para. 4; Parliamentary Assembly of the Council of Europe Recommendation 1762 (2006); Magna Charta Universitatum 1998; UNESCO Recommendation 1997; American Association of University Professors (AAUP) 1915, p. 5; Bergan and Harkavy 2020, p. 20.

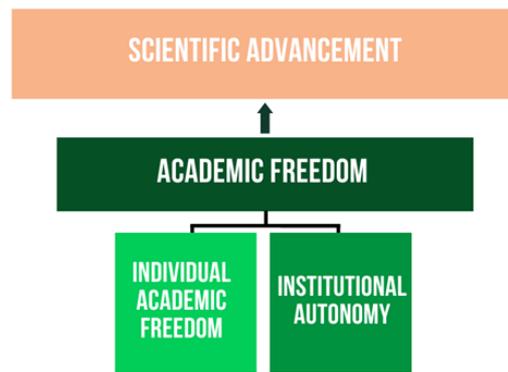


Image 3. Core academic values and their relation to each other

2.2.1 *Scientific advancement*

Scientific advancement is an intriguing concept. The first time it was introduced in an international human rights instrument was in 1948, in Article 27(1) of the Universal Declaration of Human Rights (UDHR), which laid down the right of everyone “to share in scientific advancement and its benefits.”¹²³ In 1966, a similar right was codified in Article 15(1)(b) of the International Covenant on Economic, Social and Cultural Rights (ICESCR), granting everyone the right “to enjoy the benefits of scientific progress and its applications”.¹²⁴ The right to *enjoy the benefits* of scientific advancement, or progress is nowadays considered as one of the main components of the broader “right to science”, which, notably, also encompasses the right to *participate* in scientific progress.¹²⁵ At the time of drafting the UDHR and ICESCR, however, the meaning of scientific advancement/progress was not explained, even though countries clearly held different opinions on what constitutes ‘progress’ and what does not.¹²⁶ An answer to this question was only recently provided by the UN Committee on Economic, Social and Cultural Rights (CESCR). In a General Comment, the Committee stated that both scientific advancement and scientific progress “emphasize the capacity of science to contribute to the well-being of persons and humankind” and that “the development of science in the service of peace and human rights should be prioritized by States over other uses”.¹²⁷ In other words, the CESCR takes the view that scientific advancement implies the advancement of humankind.¹²⁸ This anthropocentric conception of scientific advancement connects well with universities’ public mandate to serve society with their scientific endeavours (section 2.1).¹²⁹

Related concept: open science

¹²³ United Nations (General Assembly), *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III).

¹²⁴ United Nations (General Assembly), *International Covenant on Economic, Social and Cultural Rights*, Treaty Series, 16 December 1966, Treaty Series, Vol. 993, p. 3.

¹²⁵ CESCR General Comment No. 25, para. 11; Van Daalen 2022, p. 234-235.

¹²⁶ Smith 2020, p. 1164-1165; Van Daalen 2022, p. 234.

¹²⁷ CESCR General Comment No. 25, para. 6. In this paragraph, the CESCR seems to suggest that the “development” of science is a separate concept from the “advancement” of science, implying that when scientific development is used for the good – i.e., peace and human rights, the well-being of persons and humankind – scientific development can be regarded as scientific *advancement*. However, in paragraph 14 of the General Comment, the CESCR explicitly puts “advancement” on a par with “development”.

¹²⁸ Whether it is correct to define scientific advancement by its contribution to the advancement of humankind can however be debated. Does scientific development for its own sake not amount to “advancement”? While the development of Artificial Intelligence (AI) is not in all cases beneficial to humankind, given AI’s potential to e.g., drive people out of jobs or contribute to a totalitarian surveillance state, it does unlock humanity’s ability to explore and understand what has not been known before, which could in itself be considered as “advancement”.

¹²⁹ Or as it has been put in literature: “The university is emblematic of humanity’s quest for survival”, see Steele and Rickards 2021, p. 70.

An important precondition for scientific advancement is that scientific knowledge and its applications are widely disseminated so as to enable researchers to build on existing knowledge.¹³⁰ Viewing science as a common good, the influential American sociologist Merton considered that science should be done by society and for society. He believed that research findings are “a product of social collaboration” which should be “assigned to the community” and become “part of the public domain”.¹³¹ He argued that in order to advance the boundaries of knowledge, research findings must be fully and openly communicated.¹³² Although the idea of diffusing science is hardly new,¹³³ the call for “open science” has become particularly strong over the past two decades in parallel with the growth of the Internet and other digital technologies underpinning the modern dissemination of knowledge.¹³⁴ According to the UNESCO definition, open science can be understood as “an inclusive construct that combines various movements and practices aiming to make multilingual scientific knowledge openly available, accessible and reusable for everyone, to increase scientific collaborations and sharing of information for the benefits of science and society, and to open the processes of scientific knowledge creation, evaluation and communication to societal actors beyond the traditional scientific community”.¹³⁵ Whether it concerns publications, research data,¹³⁶ software or other digital outputs, the goal of open science is to render all those sources free for anyone to access, modify and share, subject at most to conditions that preserve provenance (e.g., attribution requirements) and openness (e.g., requirements to include the original source).¹³⁷ Effective digital infrastructures play a key role in the pursuit of open science.

2.2.2 Academic freedom

Frequently mentioned in legal and declaratory documents as an essential value undergirding universities’ public mission to pursue scientific advancement, is academic freedom. The value has been explicitly codified at the EU level in (the second sentence of) Article 13 of the Charter of Fundamental Rights of the European Union (CFREU or ‘the Charter’).

In the case of *European Commission v. Hungary*, the Court of Justice of the European Union (CJEU) recently held that the concept of academic freedom must be understood broadly and has two dimensions: an individual and an institutional one.¹³⁸ Affirming the strong connection between academic activities and

¹³⁰ Van Daalen 2022, p. 240.

¹³¹ Merton 1942, p. 121-122.

¹³² Ibid.: “Full and open communication [is] its enactment”.

¹³³ See e.g., Article 15(2) ICESCR, which since 1966 obliges States to promote the diffusion of science to achieve the full realisation of the right to science. See also CESCR General Comment No. 25, para. 61, which explicitly states that (intellectual property) restrictions on the *sharing* of information on scientific research hinder the advancement of science. See also Finkin and Post 2009, p. 69 and Merton 1942, p. 122.

¹³⁴ ALLEA Statement on Open Access, 12 December 2022.

¹³⁵ UNESCO Recommendation 2021, p. 7, para. 6.

¹³⁶ Research data may include statistics, results of experiments, measurements, observations resulting from fieldwork, survey results, interview recordings and images, see recital 27 of the Open Data Directive (1024/2019).

¹³⁷ This is the ‘Open Definition’ as formulated by the Open Knowledge Foundation, see <http://opendefinition.org/od/2.1/en/>.

¹³⁸ CJEU 6 October 2020, C-66/18 (*European Commission v. Hungary*), para. 226-227 (“...from which it is apparent that *academic freedom also incorporates an institutional and organisational dimension*, a link to an organisational structure being an essential prerequisite for teaching and research activities”). In this case, the Court followed the Opinion of A-G Kokott of 5 March 2020, in which the A-G argued that “the university serves as a platform for academic discourse and a network and infrastructure”, which is why “affiliation with a State or private university is, in practice, an essential condition for academic research” (para. 146). According to the A-G, the right to academic freedom as enshrined in Article 13 CFREU “includes not only substantively autonomous research and teaching that is free from State interference, but also its institutional and organisational framework [underpinning research and teaching]” (para. 146). See also in this regard: De Cock and Timbermont 2021; A-G Mengozzi 23 January 2014, Opinion in case C-15/13, para. 73; UN Special Rapporteur Kaye 2020, para. 9; Committee of Ministers of the Council of Europe, Recommendation CM/Rec(2012)7, para. 5; Leiden Principles, p. 3; Joint concurring opinion of Judges Sajó, Vucinic and Kuris in ECtHR 27 May 2014, Appl. No. 346/04 and 39779/04, *Mustafa Erdogan and Others v. Turkey*: (“However, although academic freedom refers, first and foremost, to institutional autonomy, it cannot be reduced to its institutional setting, since scholars’ institutional autonomy is meaningful only if they enjoy personal freedom of research...”); European Commission COM(2022) 16 final, p. 10 (“Academic freedom cannot be isolated from institutional autonomy...”); Proposition de Résolution Européenne sur un nécessaire soutien à la liberté académique en Europe, p. 14 (recital 33); and Vrielink et al 2023, p. 9 (“Less common than the individual rights approach, is the one that sees academic freedom as a right with collective dimensions, belonging to institutions (universities, faculties, etc.) rather than to individuals).

organisational structures,¹³⁹ the CJEU held that Hungary's restrictive legislation imposing conditions for the supply of higher education services within its territory "depriv[ed] [foreign] universities [...] of the autonomous and organisational structure that is necessary for conducting their academic research and for carrying out their educational activities".¹⁴⁰ As a result, the academic freedom of the affected university as protected in Article 13 of the Charter was limited.¹⁴¹ The Court did not make explicit *whose* academic freedom was limited in this context – that of the university or that of the university staff, or perhaps both¹⁴² – but the Court's explicit quotation of the UNESCO Recommendation concerning the status of higher-education teaching personnel of 1997, in which autonomy has been defined as "the institutional form of academic freedom", seems to suggest that the Court deems both individuals and institutions eligible subjects to enjoy academic freedom.¹⁴³ This multidimensionality connects well with the Humboldtian research university model of *Lehrfreiheit*, *Lernfreiheit* and *Freiheit der Wissenschaft*, the three elements of which are widely considered as the basis for the modern concept of academic freedom.¹⁴⁴

Importantly, some legal instruments and declarations analysed for this report consider the institutional dimension of academic freedom as an independent normative value, connected with but apart from academic freedom, referred to as "institutional autonomy".¹⁴⁵ In this view, academic freedom is reserved exclusively to protect individual teachers, researchers and students rather than organisations.¹⁴⁶ In line with these sources – while however still upholding the CJEU's multifaceted interpretation of academic freedom – this report also distinguishes between 'individual academic freedom', referring to the personal freedom of academics to carry out activities relating to research and teaching; and 'institutional autonomy', referring to the freedom of academic institutions to independently govern their organisations in support of research and teaching (see Image 4). For the purposes of this research project, the individual academic freedom of students to receive education is not explored further.

¹³⁹ CJEU 6 October 2020, C-66/18 (*European Commission v. Hungary*), para. 227.

¹⁴⁰ *Ibid.*, para. 228

¹⁴¹ *Ibid.*

¹⁴² Para. 220 ("Hungary contends, with regard to academic freedom, that the fact that a higher education must meet certain legal obligations does not affect the *academic freedom of the institution concerned nor that of its staff*") and para. 228 ("Consequently, those measures are such as to limit *the* academic freedom protected in Article 13 of the Charter").

¹⁴³ *Ibid.* para. 227. Notably, some authors do not read a confirmation in the Court's judgment that academic freedom protects both individuals and institutions/organisations. Maassen et al, for instance, view individual academic freedom as "the essence of academic freedom", while institutional autonomy is one of "the conditions necessary for guarding or guaranteeing academic freedom", alongside other conditions such as self-governance, labour conditions and financial conditions. See Maassen et al (STOA, European Parliament) 2023, p. 3, 8, 13-14.

¹⁴⁴ Roughly speaking, *Lehrfreiheit* refers to the freedom of academic staff to teach, conduct research and report findings in lecture or in published form without administrative restraints. *Lernfreiheit* provides students with the freedom to receive education and learn, free from universities' control over their course of study and private life. *Freiheit der Wissenschaft* refers to the freedom of academic institutions to govern themselves and control their internal affairs,¹⁴⁴ which is deemed necessary not only for its own sake but also as a means to protect the *Lehrfreiheit* of academic teachers and researchers working at the institutions. See Karran 2009a, p. 267; Metzger 1987-1988, p. 1269-1270; Metzger 1955, p. 386; Horwitz 2005, p. 475; and Karran and Beiter 2020, p. 123.

¹⁴⁵ E.g., CESCR General Comment No. 13, para. 40; UNESCO 1997, para. V.A.17, V.A.20, V.A.27; Parliamentary Assembly of the Council of Europe, Recommendation 1762 (2006), para. 4.2; Committee of Ministers of the Council of Europe, Recommendation CM/Rec(2012)7, para. 6; European Parliament 2018/2117 (INI), p. 6, sub-para. n; World University Service Lima Declaration 1988, Preamble, para. 1(c), para. 17, 19; Joint Statement by ALLEA, EUA and Science Europe 2019; European University Association (EUA) Lisbon Declaration 2007, p. 6, para. 26. In literature, see e.g., De Groof 2010, p. 8-9 and Wolf 2000, p. 198.

¹⁴⁶ The Royal Netherlands Academy of Arts and Sciences (KNAW) 2021, p. 22, 30: "The Academy defines academic freedom as the principle that employees working at scientific institutions can freely conduct their scientific research, communicate their findings and provide education." See also *Kamerstukken II* (Dutch legislative history) 1990-1991, 21 073, nr. 17, p. 39: "Academic freedom can be described as a right closely related to the freedom of opinion and expression and specifically aimed at the position of individual teachers, researchers and students".



Image 4. Academic freedom as a multidimensional umbrella right

As two sides of the same coin, individual academic freedom and institutional autonomy are closely related concepts. Institutional autonomy is generally perceived as a “supportive element”¹⁴⁷ to ensure individual academic freedom, or as the US Supreme Court once put it: “academic freedom thrives [...] on autonomous decision making by the academy itself”.¹⁴⁸ Some legal and declaratory documents consider institutional autonomy even as a “necessary precondition”¹⁴⁹ for individual academic freedom, pointing out that the institutional framework creates and guards the conditions under which individual academic freedom can be optimally exercised.¹⁵⁰ This does not mean, however, that individual and institutional autonomy always reinforce one another. In the *Lombardi*-case,¹⁵¹ for example, a university and a lecturer faced each other in a conflict over the lecturer’s teaching position at the institution. The Christian university considered some of the lecturer’s views to be “in clear opposition to the Catholic doctrine”¹⁵² and therefore refused to renew the lecturer’s contract. The European Court of Human Rights (ECtHR) ultimately held that in this case, the procedural guarantees afforded by the right to academic freedom of the individual lecturer outweighed the autonomy of the university to provide education inspired by Catholic doctrine.¹⁵³

The remainder of this section will now focus on the meaning of individual academic freedom. In doing so, a distinction is made between the activities that require protection (freedom “to”), and the forces against which protection is sought (freedom “from”). Subsequently, the meaning of institutional autonomy will be explained in the next section.

Freedom “to”: protected activities

In Europe, individual academic freedom is typically considered a species of the general right to freedom of expression and information tailored to members of the academic community.¹⁵⁴ It is interpreted broadly as

¹⁴⁷ Karan and Beiter 2020, p. 125. See also EUA, ALLEA and Science Europe Joint Statement 2019 (“underpinning”), Annex I to the EHEA Rome Ministerial Communiqué 2020, p. 3 (“constitutive for”, “intricately related to”) and GPPI 2021, p. 6 (“key element in the de facto realization of academic freedom”).

¹⁴⁸ U.S. Supreme Court, *University of Michigan v. Ewing*, 474 U.S. 214 (1985), footnote 12, with reference to *University of California Regents v. Bakke*, 438 U.S. 265, 438, U.S. 32 (1978). See also Association of American Universities (AAU) 2013, p. 2.

¹⁴⁹ UNESCO Recommendation 1997, para. V.A.18, p. 52 and World University Service Lima Declaration 1988, preamble. See also CJEU 6 October 2020, C-66/18 (*European Commission v. Hungary*), para. 227 (“essential prerequisite”); CESCR General Comment No. 13 1999, para. 40 (“requires”); Vrielink et al. 2023, p. 4 (“sine qua non”); World University Service Lima Declaration 1988, para. 18 (“demand”); Deca 2020, p. 156 (“sine qua non precondition”).

¹⁵⁰ Maassen et al (STOA, European Parliament) 2023, p. 4, referring to Beaud 2022, p. 213.

¹⁵¹ ECtHR 20 October 2009, App. No. 39128/05 (*Lombardi*), paras. 47, 52, 55.

¹⁵² Information Note on the Court’s case-law No. 123, <<https://hudoc.echr.coe.int/eng?i=002-1276>>.

¹⁵³ ECtHR 20 October 2009, Appl. No. 39128/05 (*Lombardi*), para.55.

¹⁵⁴ E.g., the Explanatory Memorandum to Article 13 of the Charter of Fundamental Rights of the European Union (CFREU), stating that the freedom of arts and science “is deduced primarily from the right to freedom of thought and expression.” See also

encompassing a) academics' freedom of scientific research, b) freedom of teaching, as well as c) their freedom to express freely their views and opinions in the areas of their research, professional expertise and competence,¹⁵⁵ both inside and outside the university sector.¹⁵⁶ The freedom of science, on the one hand, is firmly cemented in international and European law,¹⁵⁷ protecting researchers¹⁵⁸ against undue influence on their independent judgment and enabling them to inter alia set up autonomous research institutions; define the aims and objectives of the research and the methods to be adopted; choose and develop theories; gather empirical material; freely and openly question the ethical value of certain projects; withdraw from those projects if their conscience so dictates; cooperate with other researchers both nationally and internationally; share scientific data and analysis with policymakers and the public; question accepted wisdom; and develop new ideas.¹⁵⁹ The freedom of teaching, on the other hand, is less articulated in legal and declaratory documents but is generally understood as the freedom of teachers to determine the contents and methods of their teaching¹⁶⁰ and to express scientific views they deem correct.¹⁶¹ Last but not least, the freedom of academics to express and communicate freely their views and opinions empowers them to speak out about matters related or unrelated to the narrow subject of their professional scholarship,¹⁶² for example about the institution or system in which they work¹⁶³ or about societal issues, e.g., in the form of an expert contribution to public debate.¹⁶⁴ In a nutshell, individual academic freedom aims to protect all activities carried out by academics relating to the pursuit, development and transmission of knowledge and ideas.¹⁶⁵ Any restrictions on the freedom of academics to carry out such activities must be submitted to careful scrutiny.¹⁶⁶

Freedom “from”: threats

the Declaration adopted at the Global Forum on Academic Freedom, Institutional Autonomy and the Future of Democracy 2019, para. 5 and the Leiden Principles p. 3, first bullet point. Moreover, cases concerning academic liberties brought before the ECtHR are commonly dealt with on the basis of Article 10, which protects the general right to freedom of expression and information, see Timbermont 2022. See also the Proposition de Résolution Européenne sur un nécessaire soutien à la liberté académique en Europe, p. 5, which describes how the ECHR only protects academic freedom as an “avatar” of the freedom of expression. A recurring phrase in the ECtHR's case law is that academic freedom “should guarantee freedom of expression and of action, freedom to disseminate information and freedom to conduct research and distribute knowledge and truth without restriction”, see ECtHR 23 June 2009, Appl. No. 17089/03 (*Sorguc v. Turkey*), para. 21; ECtHR 20 October 2009, Appl. No. 39128/05 (*Lombardi*), para. 43; ECtHR 27 May 2014, Appl. No. 346/04 (*Mustafa Erdogan and Others v. Turkey*), para. 40; and ECtHR 19 June 2018, Appl. No. 20233/06 (*Kula v. Turkey*), para. 38. This particular phrase is derived from Recommendation 1762 (2006) of the Parliamentary Assembly of the Council of Europe on Academic freedom and university autonomy.

¹⁵⁵ ECtHR 27 May 2014, Appl. No. 346/04 (*Mustafa Erdogan and Others v. Turkey*), para. 40. This triad of research, teaching and freedom of expression/communication has also been endorsed in literature, see e.g., Beaud 2022, p. 216-217, followed by Maassen et al (STOA, European Parliament) 2023.

¹⁵⁶ Annex I to the EHEA Rome Ministerial Communiqué 2020, p. 3.

¹⁵⁷ Article 15(3) ICESCR; Article 13 CFREU.

¹⁵⁸ N.B. The freedom of scientific research does not only apply to academic researchers but also to research conducted by non-academics, including researchers working at private companies.

¹⁵⁹ CESCR General Comment No. 25 (2020), para. 13 on Article 15(3) ICESCR. See also the Bonn Declaration 2020, p. 2. See also the Dutch legislator in *Kamerstukken II* (Dutch legislative history), 1980-1981, 16 802, nr. 3, p. 49-50, stating that researchers are free to “initiate the research theme” and to “follow their own insights” within the framework of societal, ethical, scientific and faculty norms. N.B. Researchers are free to publish their findings both in academic circles and in the economic sphere, see ECtHR 25 August 1998, Appl. No. 59/1997/843/1049 (*Hertel v. Switzerland*), para. 44, 50; *Kamerstukken II*, 1990-1991, 21 073, nr. 17 (Vierde Nota van Wijziging), p. 39 and *Kamerstukken II*, 1980-1981, 16 802, nr. 3, p. 49-50.

¹⁶⁰ *Kamerstukken II* (Dutch legislative history), 1980-1981, 16 802, nr. 3, p. 49-50; see also American Association of University Professors (AAUP) 1940, p. 14, para. 2.

¹⁶¹ *Kamerstukken II* (Dutch legislative history), 1980-1981, 16 802, nr. 3, p. 49-50.

¹⁶² Compare Finkin and Post 2009, p. 73.

¹⁶³ For instance, about institutional actions, decisions or policies (intra-mural expression). See ECtHR 23 June 2009, Appl. No. 17089/03 (*Sorguc v. Turkey*), para. 21; ECtHR 15 April 2014, Appl. No. 40877/07 (*Hasan Yazici v. Turkey*), para. 55. See also UNESCO Recommendation concerning the status of higher-education teaching personnel (1997), para. V.A.27; CESCR General Comment No. 13, para. 39.

¹⁶⁴ McGonagle 2021, para. 15. Such opinions and views may include, for example, an examination or criticism of the functioning of public institutions in a given political system (extra-mural expression), see also ECtHR May 2014, Appl. No. 346/04 (*Mustafa Erdogan and Others v. Turkey*), para. 40.

¹⁶⁵ CESCR General Comment No. 13, para. 39.

¹⁶⁶ ECtHR 15 March 2012, Appl. Nos. 4149/04 and 41029/04 (*Aksu v. Turkey*), para. 71.

The reviewed legal and declaratory sources indicate that individual academic freedom is primarily interpreted as a ‘negative’ freedom, meaning that academics must be protected from control and restraints exercised by third parties, especially the State¹⁶⁷ but also private-sector actors (notably, non-legal declarations tend to assume horizontal application of the right to academic freedom).¹⁶⁸ In the specific context of scientific evaluation, it could be argued that individual academic freedom implies that the work of academic researchers may not be subject to review by the State or the private sector, but solely by disinterested fellow academics (peer-review).¹⁶⁹ Limitations of individual academic freedom in the negative sense include acts of intimidation, repression, censorship, (threats of) disciplinary action or dismissal, discrimination, imprisonment and other forms of undue outside interference preventing or deterring academics from performing the activities described above.¹⁷⁰

Additionally, in legal literature it has been suggested that academic freedom also has a ‘positive’ dimension (not to be confused with positive state obligations, see section 2.2.4). In this view, academics should not only be free from control by others, but also be free to control themselves. The positive conception of academic freedom is centred around the notion of self-determination, i.e., the ability of academics to pursue their work in ways they deem appropriate (in keeping with disciplinary norms) and to be free from being required to do things.¹⁷¹ Interferences with academic freedom, when interpreted as a positive freedom, could result from external obligations and requirements which – although perhaps not directly infringing with the exercise of academic activities as such – conflict with researchers’ self-determined course of action. Whether or when such external obligations could indeed *violate* the right to academic freedom does not yet follow from (soft) law nor literature. After all, academic freedom does not imply that academics are completely free from any form of restraint.¹⁷²

Related concepts: freedom of assembly and association, freedom of movement, right to privacy/data protection

Individual academic freedom has inherently strong linkages with other human rights. Besides the right to freedom of expression, one could also think of the freedom of assembly and association (e.g., to form scientific associations or organise conferences and symposia), the freedom of movement (e.g., to visit conferences and carry out fieldwork) and the rights to privacy and data protection. Researchers need autonomous and private spaces to conduct their research, in which they are free from “prying eyes”¹⁷³ or surveillance by the State or

¹⁶⁷ Notably, the Charter of Fundamental Rights of the European Union (CFREU) applies to Member States only when they are implementing Union Law, see Article 51 CFREU. For example, in the case of *European Commission v. Hungary* (CJEU 6 October 2020, C-66/18), the Court of Justice held that Hungary was implementing Union law when performing obligations under the so-called GATS agreement and therefore had to comply with the fundamental rights enshrined in the Charter, see para. 213.

¹⁶⁸ *Magna Charta Universitatum* 1988, Principle 1 (“morally and intellectually independent of all political authority and economic power”); Report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (David Kaye) 2020, para. 17 (“not subject to interference, such as intimidation and harassment”); CESCR, General Comment No. 25, para. 13 (free from “undue influence”); UNESCO Recommendation concerning the status of higher-education teaching and personnel 1997, para. V.A.27 (“without constriction by prescribed doctrine”, “freedom from institutional censorship” and “without discrimination of any kind and without fear of repression by the state or any other source”); American Association of University Professors (AAUP) 1940, p. 14 (free from “institutional censorship”); Committee of Ministers of the Council of Europe, Recommendation CM/Rec(2012)7, para. 5 (free from “undue outside interference, by public authorities or others” and “without the fear of disciplinary action, dismissal or any other form of retribution”); Parliamentary Assembly of the Council of Europe, Recommendation 1762 (2006), para. 4.1 (“without restriction”); Dar es Salaam Declaration 1990, para. 19-20 and World University Service Lima Declaration 1988, para. 6-7 (“without [any] interference”); Dar es Salaam Declaration 1990, para. 19-20 (“not hindered in any way”); International Association of Universities (IAU) policy statement 1998, para. 2 (“without outside pressure”); CESCR, General Comment No. 13, para. 39 and UNESCO Recommendation concerning the status of higher-education teaching and personnel 1997, para. V.A.27 and World University Service Lima Declaration 1988, para. 3 (“without discrimination or fear or repression by the State or any other actor”); Annex I to the EHEA Rome Ministerial Communiqué 2020, p. 3 (“without fear of reprisal”); Dutch legislator in *Kamerstukken II* (Dutch legislative history), 1980-1981, 16 802, nr. 3, p. 49-50 (“independent from certain political, philosophical or scientific-theoretical views”).

¹⁶⁹ Goldenfein and Griffin 2022, p. 9, with reference to Bourdieu 2004, p. 54.

¹⁷⁰ See quotes in *supra* note 169.

¹⁷¹ Johnston 2017, with reference to Berlin 1969.

¹⁷² Finkin and Post 2009, p. 59.

¹⁷³ Aspesi et al (SPARC) 2019b, p. 7.

other actors. Only then, researchers can truly develop and follow their own insights, challenge paradigms and work on sensitive or ‘taboo’ topics.¹⁷⁴ Surveillance and monitoring of research practices can lead to a culture of self-censorship and significant scientific work not being carried out.¹⁷⁵ Academics’ privacy is therefore an important gateway to the effective enjoyment of academic freedom.¹⁷⁶

2.2.3 Institutional autonomy

In the words of EU Advocate-General Kokott, universities function as “platform[s] for academic discourse”.¹⁷⁷ Given universities’ essential role in enabling academic research and education, their autonomous organisational structure that is used to govern these activities must be duly protected.¹⁷⁸ Again, a distinction can be made between university operations that require protection (autonomy “to”) and the forces against which protection is sought (autonomy “from”).

Autonomy “to”: protected activities

Institutional autonomy traditionally aims to ensure a certain “degree of self-governance necessary for effective decision-making by institutions of higher education”.¹⁷⁹ The decisions for which self-governance is envisaged can be grouped in two categories: first, decisions regarding academic research and teaching as such,¹⁸⁰ and second, decisions regarding administrative matters that enable academic research and teaching.¹⁸¹ The second category can in turn be divided into *financial* decisions, *organisational* decisions and *staffing* decisions.¹⁸² In addition, it could be argued that universities should also have the autonomy to make *economic* decisions.¹⁸³ Economic autonomy refers to the capacity of an entity to make independent decisions

¹⁷⁴ ARTICLE 19 Policy Brief 2017, p. 4; see also Dab 2022, in: LERU New Year’s Debate 2022 (01:26:55 and further).

¹⁷⁵ Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (David Kaye) 2020, para. 48, referencing Taştan and Ördök 2020, p. 117 (explaining how state monitoring of research renders researchers unproductive and engaging in self-censorship).

¹⁷⁶ Compare Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, (David Kaye) 2015, para. 16-18 with reference to UN General Assembly Resolution 68/167, A/HRC/13/37, para. 14.

¹⁷⁷ A-G Kokott, Opinion for case C-66/18 (*European Commission v. Hungary*) of 5 March 2020, para. 146.

¹⁷⁸ CJEU 6 October 2020, C-66/18 (*European Commission v. Hungary*), para. 226-228.

¹⁷⁹ UNESCO 1997, para. V.A.17 and CESCR General Comment No. 13, para. 40.

¹⁸⁰ Committee of Ministers of the Council of Europe, Recommendation CM/Rec(2012)7, para. 6. See also UNESCO 1997, para. V.A.17 and CESCR General Comment No. 13, para. 40 (“academic work”); the Report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (David Kaye) 2020, para. 12 (“pedagogical functions”); Partly dissenting opinion of Judge Pinto in ECtHR 2 April 2013, Appl. Nos. 25851/09, 29284/9 and 64090/09, *Tarantino and Others v. Italy* (“establishment of the academic curriculum”); and World University Service Lima Declaration 1988, Preamble, para. 1(c), para. 17, 19 (“determination of policies of education, research, extension work and other related activities”).

¹⁸¹ E.g., World University Service Lima Declaration 1988, Preamble, para. 1(c), para. 17, 19 (“internal government, finance, administration” and “the selection of academic and administrative staff”); UNESCO 1997, para. V.A.17 and CESCR General Comment No. 13, para. 40 (“standards, management and related activities”); Report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (David Kaye) 2020, para. 12 (“administrative, financial and disciplinary functions”); Parliamentary Assembly of the Council of Europe, Recommendation CM 1762 (2006), para. 4.2 (“beneficial policy, good governance and efficient management”); Partly dissenting opinion of Judge Pinto in ECtHR 2 April 2013, Appl. Nos. 25851/09, 29284/9 and 64090/09, *Tarantino and Others v. Italy* (“admission, evaluation, suspension and expulsion of students”); Spanish Organic Law 6/2001 on Universities, Article 2(2)(b) (“the selection and promotion of academic and administrative staff” and “the budget and financial organization of the institution”, “the election, designation and removal of governing and representative bodies” and “the issuing of university qualifications of an official and legal nature”); and CRVB 10 January 2019, ECLI:NL:CRVB:2019:51, para. 2 (“the structure of the organisation”).

¹⁸² See the taxonomy as introduced by the European University Association (EUA) in 2007, which distinguishes between four key dimensions of autonomy, namely: academic autonomy (decisions relating to e.g., curricula, research), financial autonomy (decisions relating to e.g., borrowing funds, budgeting, tuition fees), organisational autonomy (decisions relating to e.g., university structure, leadership, governance) and staffing autonomy (decisions relating to e.g., recruitment, salaries and promotion). See also European University Association (EUA) Lisbon Declaration 2007, p. 6, para. 26 and Bennetot Pruvot, Estermann and Popkhadze 2023, p. 9.

¹⁸³ E.g., Spanish Organic Law 6/2001 on Universities, Article 79(1), <<https://www.boe.es/buscar/pdf/2001/BOE-A-2001-24515-consolidado.pdf>>.

about its economic future.¹⁸⁴ This means that it should be able to establish and maintain economic relations with other organisations¹⁸⁵ and to achieve economic aspirations (for instance the commercialisation of research results).¹⁸⁶ A precondition for economic autonomy is that universities have sufficient (monetary) resources at their disposal¹⁸⁷ and are resilient to non-competitive market structures and practices (see below).

At the level of EU Member States, the Spanish Law 6/201 on Universities in particular provides an elaborate, yet non-exhaustive¹⁸⁸ list of decisions that universities should be able to take autonomously. This open-endedness of autonomous decision-making connects well with the view of the Committee of Ministers of the Council of Europe that “institutional autonomy should be a dynamic concept evolving in the light of good practice”.¹⁸⁹ From this perspective, it could be argued that “infrastructural autonomy”,¹⁹⁰ i.e., the capability of universities to (co-)decide how digital services are developed and on the basis of which standards, has become a new relevant dimension of institutional autonomy in the digital age.

Autonomy “from”: threats

According to the analysed sources, the biggest threats to university autonomy originate from state authorities and the commercial sector. Universities must remain independent from “undue pressure from state and business interests”;¹⁹¹ “the State and all other forces of society”;¹⁹² “political authority and economic power”;¹⁹³ “political and economic interference”;¹⁹⁴ “state, business or other non-state actors’ interference or attacks”;¹⁹⁵ as well as from “politicisation and ideological manipulation”.¹⁹⁶ It is further emphasised “that all institutions of higher education should strive to prevent scientific and technological dependence”.¹⁹⁷

Related concepts: competitive market structures and practices

One of the threats to institutional autonomy most felt by universities in the digital realm is that of non-competitive structures and practices in the markets for digital services. Even though many European universities are publicly funded and, as public entities, subject to procurement rules, in the pursuit of their activities they transact with commercial digital service providers just as any other market actors. The economic relations with such providers are often imbalanced due to information and power asymmetries in favour of commercial actors, which lead to economic dependencies and inefficiencies. The asymmetries felt in the digital realm are typically the result of non-competitive market structures (oligopolies) and practices (e.g., service bundling) that tend to weaken buyers’ negotiating positions and create risks for price, quality and innovation.¹⁹⁸ In the university context, economic dependencies and inefficiencies resulting from these asymmetries undermine the economic autonomy of academic institutions. This is objectionable, since universities’ autonomy from undue impact of non-competitive market structures and practices is an important precondition for universities’ ability to make independent decisions regarding the digital products and services they purchase

¹⁸⁴ Sarooshi 2004, p. 656.

¹⁸⁵ Compare Article 2(2)(j) of the Spanish Organic Law 6/2001 on Universities.

¹⁸⁶ Compare Häyriinen-Alestalo and Peltola 2006, p. 266.

¹⁸⁷ E.g., Spanish Organic Law 6/2001 on Universities, Article 79(1).

¹⁸⁸ Article 2(2)(k) of the Spanish Organic Law 6/2001 leaves room for “any other functions necessary for the appropriate fulfilment of the [university] functions indicated in paragraph 2 of article 1.”

¹⁸⁹ Committee of Ministers of the Council of Europe, CM/Rec(2012)7, para. 6.

¹⁹⁰ Poell, in KNAW Expertmeeting IV 2022, 18:09 and further.

¹⁹¹ World University Service Lima Declaration 1988, Preamble.

¹⁹² *Ibid.*, para. 1(c).

¹⁹³ Magna Charta Universitatum 1988, Principle 1.

¹⁹⁴ Joint Statement by ALLEA, EUA and Science Europe 2019, p. 1.

¹⁹⁵ European Parliament 2018/2117 (INI), p. 6, sub-para. n.

¹⁹⁶ *Ibid.*

¹⁹⁷ World University Service Lima Declaration 1988, Preamble, para. 17.

¹⁹⁸ ACM Market Study Cloud Services 2022, p. 6.

from commercial actors in support of their research, teaching and administration activities.¹⁹⁹ This particular form of autonomy is, therefore, instrumental to safeguarding the universities' wider institutional autonomy.

2.2.4 Protection and promotion of academic values

In the reviewed documents, the protection and promotion of academic values is mainly regarded as a joint endeavour of public authorities, universities, the academic community and other stakeholders.²⁰⁰ Universities, for instance, may not use their institutional autonomy “as a pretext”²⁰¹ to limit the rights of academic staff. Instead, they must provide “effective support”²⁰² of academic freedom and adopt policies to ensure the free expression rights of the members of their communities.²⁰³ Public authorities, however, have a heightened responsibility in this regard. According to international human rights law, states have a legal obligation to take “those steps necessary for the development of science.”²⁰⁴ This means that they not only have a negative duty to refrain from actions which could hinder people to participate in science, but also a positive duty “to actively promote the advancement of science”.²⁰⁵ This positive duty requires states to approve policies and regulations that foster scientific research, to allocate appropriate resources, and more generally, to create “an enabling and participatory environment for the [...] development [...] of science”.²⁰⁶ Importantly, this duty also includes the protection and promotion of academic freedom²⁰⁷ and institutional autonomy,²⁰⁸ which in turn requires the provision of substantial public funding.²⁰⁹ Moreover, the positive obligation demands that states make (knowledge about) scientific advancement and its applications broadly available and accessible to the general public, which can be done by e.g., providing instruments for the diffusion of science, strong research infrastructures with adequate resources, and appropriate financing of scientific education.²¹⁰ Finally, it could be argued that the positive state obligation to promote scientific advancement and academic freedom implies the regulation of *private* actors whose conduct in providing assistance to academic research and teaching impairs the enjoyment of these values.²¹¹

2.3 Academic values and digital sovereignty

¹⁹⁹ Aspesi and Brand 2020, p. 574: “The healthy functioning of the academy, including fair terms and conditions from commercial partners, requires that the market for data analytics and knowledge infrastructure be kept open to real competition, within a global market place.”

²⁰⁰ E.g., International Association of Universities (IAU) 1998, para. 3 jo. 6-7; Recommendation CM/Rec(2012)7, para. 4; Declaration adopted at the Global Forum on Academic Freedom, Institutional Autonomy and the Future of Democracy 2019, para. 4 and calls for action.

²⁰¹ UNESCO Recommendation 1997, para. V.A.20. See also Recommendation CM/Rec(2012)7, para. 8 (first sentence) and Article 1.6 of the Dutch Law on Higher Education and Scientific Research (*Wet op het hoger onderwijs en wetenschappelijk onderzoek*).

²⁰² UNESCO 1997, para. V.B.22(c). See also Leiden Principles 2022, p. 3, third bullet point; Bergan and Harkavy 2020, p. 24; Scholars at Risk 2020, para. 18.

²⁰³ Report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (David Kaye) 2020, para. 12.

²⁰⁴ Article 15(2) ICESCR.

²⁰⁵ CESCR General Comment No. 25 (2020), para. 46.

²⁰⁶ Ibid.

²⁰⁷ Ibid.

²⁰⁸ UNESCO Recommendation (1997), V.A.19; World University Service Lima Declaration (1988), para. 18; see also UN Special Rapporteur 2018, p. 6: “States are under a positive obligation to create a general enabling environment for seeking, receiving and imparting information and ideas. Institutional protection and autonomy are a part of that enabling environment.”

²⁰⁹ Recommendation CM/Rec(2007)6, para. 16-17; Declaration adopted at the Global Forum on Academic Freedom, Institutional Autonomy and the Future of Democracy 2019, call for action on public authorities (4th bullet point).

²¹⁰ CESCR General Comment No. 25 (2020), para. 16, 47.

²¹¹ Compare the Abidjan Principles 2019, para 58 and 77.

In step with the digitalisation and datafication of universities (Chapter 1), the core academic values as explained in the previous sections not only apply to the physical but also to the digital world. Many of the activities carried out by universities and academics nowadays involve digital tools and data. It is therefore necessary that academic freedom and institutional autonomy, and universities' public-interest mission to contribute to scientific advancement more generally, are strongly protected and promoted in the digital domain as well. This, as noted in the beginning of this Chapter, requires that universities and academics possess a minimum level of digital sovereignty. Alternatively stated, digital sovereignty is a mechanism and necessary precondition to safeguard academic values in the digital age (Image 5).

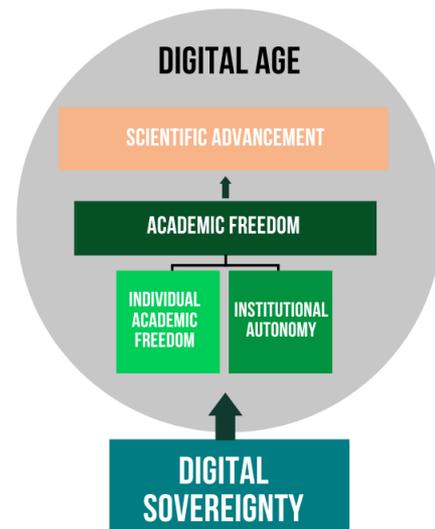


Image 5. Digital sovereignty as a necessary precondition to safeguard academic values in the digital age

3. Digital sovereignty claims in the university context

The academic community has started to realise that universities’ digital operations heavily rely on commercial providers of digital infrastructures and data services. While reliance on external parties is not new, the scale and scope of universities’ integration with digital providers has reached unprecedented levels. Against this background, representatives of the university sector have voiced their concerns about universities and academics’ diminishing control over digital infrastructures and data.²¹² This Chapter will review such statements and discuss their merits. In doing so, it follows the model for digital sovereignty in the university context introduced in the first Chapter, thus defining digital sovereignty claims made in the university context by identifying threats to academic values. The last section reflects on universities’ responsibility and agency to address digital sovereignty claims by themselves (for example by harnessing procurement strategies and implementing other institutional practices) and on the situations where threats seem to be beyond universities’ power to solve.

3.1 Generic and specific digital sovereignty claims

Digital sovereignty claims can be categorised in two ways: whether they are generic (i.e., shared with other organisational actors) or specific (i.e., unique to the university context). The lists of generic and specific digital sovereignty claims presented in Tables 2a and 2b are not meant to be exhaustive but rather indicative of the most commonly identified issues. Some of the threats identified by university sector representatives are generic in the sense that they also feature in other sectors and industries – after all, the increasing power of digital technology companies is a broader societal dynamic – while others are inherently unique to the university context. Technology-and-vendor lock-ins, for instance, exist and arise in many economic sectors. The accumulation of data about research and teaching in private infrastructures, on the other hand, affects universities in particular. The distinction between generic and specific claims is made to point out where the university sector faces different problems than other economic sectors and therefore deserves special protection.

At the same time, the line between generic and specific threats, and the digital sovereignty claims emanating from those threats, cannot be drawn too sharply. Generic threats often have specific manifestations or consequences in the university context as they collide with academic values that do not apply to other industries. Surveillance of academic researchers, for example, is not just an issue of data protection as it is for other organisations, but strongly intersects with academic freedom. And the lock-in of a university by a digital technology provider is not just undesirable from the perspective of market competition and organisational self-determination, but also because it could impede free teaching, research and scientific advancement. The unique mission and function of universities in society by definition gives rise to somewhat ‘special’ digital sovereignty claims.

| Category | Digital sovereignty claims, defined by: | | Dimensions | | Actors of digital sovereignty | Direct addressees of claims |
|----------|---|------------------------------|---------------|------|-------------------------------|-----------------------------|
| | Threats | Academic values under threat | Infra-struct. | Data | | |
| | | | | | | |

²¹² ‘Representatives’ are interpreted here in a broad sense and include academics, university leaders, (representatives of) university associations, non-profit advocacy organisations, IT procurement organisations for education and research and government supervisory authorities (e.g., competition authorities).

| | | | | | | |
|--|---|--|---|---|-------------------------|----------------|
| Generic <i>Shared with other organisations and/or sectors</i> | Concentrated markets, leading to a reduction of user choice, a lack of bargaining power vis-à-vis commercial digital technology providers, and potentially technology-and-vendor lock-ins | Institutional autonomy, incl. economic autonomy; scientific advancement | X | | Universities | Tech companies |
| | Surveillance and other risks to individuals' privacy and data protection rights (e.g., cybersecurity vulnerabilities and potential access to user data by foreign governments) | Individual academic freedom, incl. privacy and data protection; scientific advancement | | X | Academics | Tech companies |
| | Extraction and exploitation of user-generated data for product refinement and development ("value capture") | Individual academic freedom, incl. privacy and data protection; institutional autonomy; scientific advancement | | X | Academics, universities | Tech companies |
| | Erosion of essential sectorial expertise, practices, norms and values due to the importing of commercial practices via techno-commercial architectures and algorithms ²¹³ | Individual academic freedom; institutional autonomy; scientific advancement | X | | Academics, universities | Tech companies |

Table 2a. Generic digital sovereignty claims

| Category | Digital sovereignty claims, defined by: | | Dimensions | | Actors of digital sovereignty | Direct addressees of claims |
|---|---|---|---------------|------|-------------------------------|-----------------------------|
| | Threats | Academic values under threat | Infra-struct. | Data | | |
| Specific <i>Unique to the university context</i> | Bundling of read-and-publish agreements and data analytics service arrangements, thus marginalising competitors and increasing the costs of switching between services | Institutional autonomy, incl. economic autonomy | X | | Universities | Tech companies |
| | Reliance on private research infrastructures limiting foundational research | Institutional autonomy; scientific advancement | X | | Universities | Tech companies |
| | Commercial influence on independent academic research and education, university decision-making and scholarship evaluation via techno-commercial architectures and algorithms | Individual academic freedom; institutional autonomy; scientific advancement | X | | Academics, universities | Tech companies |
| | Privatisation of knowledge through the accumulation of metadata about research and teaching in private-sector infrastructures | Institutional autonomy; scientific advancement | | X | Universities | Tech companies |

²¹³ For example, when during the COVID-19 pandemic the practice of 'contact tracing' in the medical sector was partly automated via an app, a concern raised in literature was that human epidemiological expertise of contact tracers, such as the ability to build trust with interviewees, provide targeted information and use skills of empathy, patience and understanding, would be "crowded out" by the introduction of app notifications, see Sharon 2020, p. 551-552.

| | | | | | |
|--|---|---|---|-------------------------|----------------|
| Difficulties to access data kept in private digital ecosystems, thus constraining certain types of scientific research | Individual academic freedom; scientific advancement | | X | Academics | Tech companies |
| Limited choice in regard to digital tools to assist in research and education | Individual academic freedom | X | | Academics | Universities |
| Instrumentalisation of publicly-funded research data for private business models | Scientific advancement | | X | Universities; academics | Tech companies |

Table 2b. University-specific digital sovereignty claims

3.2 Claims relating to digital technologies and infrastructures

Universities' increased reliance on digital technologies and infrastructures provided by commercial suppliers (Chapter 1) bears with it a series of threats to universities' infrastructural sovereignty and underlying academic values. Highlighted in this section are the risks of technology-and-vendor lock-ins and of commercial influence on independent teaching, research and university administration.

3.2.1 Concentrated markets and technology-and-vendor lock-ins

A generic threat frequently mentioned by university representatives is that the markets for digital technologies and data infrastructures are highly concentrated with only a few, mostly non-European, suppliers.²¹⁴ This market concentration leaves universities with little initial choice between providers and weakens their negotiating position.²¹⁵ On top of that, practice has shown that once universities have first committed themselves to a digital technology provider, they risk getting trapped in a "technology-and-vendor lock-in".²¹⁶ A technology-and-vendor lock-in constitutes an economic situation in which customers using certain proprietary technology have gotten 'stuck' with that specific technology and its provider (vendor) due to high barriers of switching to other providers.

Cloud services: high market concentration and almost inevitable lock-ins

The cloud services market is a perfect example of a market characterised by concentration and lock-in effects. It is currently dominated by three "hyperscalers": Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP).²¹⁷ CIOs of Dutch companies have indicated²¹⁸ that these and other large cloud providers tend to apply conditions and tariffs unilaterally, leaving no room for negotiation and undermining organisations' ability to contractually protect themselves against the consequences of lock-ins.²¹⁹ A study performed by the Dutch Competition Authority (ACM) observed that once an organisation decides to work

²¹⁴ Maex et al 2019; Maex 2021; Aspesi and Brand 2020, p. 575-576; Williamson 2020, p. 52-53, 63 (about platform capitalism in higher education); DFG Briefing Paper 2021, p. 5, 8.

²¹⁵ ACM Market Study Cloud Services 2022; see also Maex et al 2019; Bok et al (VSNU) 2021, p. 4.

²¹⁶ ACM Market Study Cloud Services 2022, p. 55.

²¹⁷ ACM Market Study Cloud Services 2022, p. 35. Other medium-sized operators active in Europe and the Netherlands are for example IBM, Oracle, VMware, OVHcloud and Scaleway, see p. 37.

²¹⁸ ACM Market Study Cloud Services 2022, p. 64.

²¹⁹ ACM Market Study Cloud Services 2022, p. 63-64; see also Aspesi and Brand 2020, p. 575-576.

with a certain cloud provider, it is extremely difficult to migrate to a new provider due to organisational, technical and financial barriers.²²⁰ Since cloud services are usually strongly interconnected with the business processes of an organisation, it takes a lot of time and effort for an organisation to ‘unbundle’ the services and reorganise them,²²¹ also taking into account that not every product is interchangeable because of incompatible product offerings.²²² Moreover, the differences between APIs and standards may complicate the technical transfer data from one cloud service to another.²²³ And even if data portability is facilitated, the high costs of transferring the data (so-called “egress fees”) may discourage users from doing so.²²⁴ Cloud service lock-ins are typically reinforced by the fact that the services of different cloud providers do often not work well together (poor interoperability), thereby complicating a multi-cloud strategy.²²⁵ Lock-ins may lead to higher prices, a reduction of service quality and innovation, and overall less favourable terms.²²⁶

From the perspective of academic values, it can be argued that concentrated markets and technology-and-vendor lock-ins infringe on universities’ institutional autonomy. First, market concentration limits universities’ *economic* autonomy to enter into commercial relationships with entities of their choice and to enforce fair terms and conditions, including reasonable pricing. Second, technology-and-vendor lock-ins threaten universities’ institutional autonomy by exposing them to continuity and portability risks. The fact that even the most high-quality digital technologies and infrastructures have vulnerabilities and security gaps²²⁷ means that universities can well become the victims of security incidents and technical malfunctions.²²⁸ If universities in such cases do not have alternative services at their disposal, they may become temporarily dysfunctional.²²⁹ Moreover, digital technology providers *themselves* could also unilaterally cancel or deliberately interrupt universities’ operations. What happens if a cloud provider, for whatever reason, would decide to “turn of the Cloud”?²³⁰ Companies that rule in oligopolistic markets and lock in customers can easily raise prices, deteriorate service levels or prioritise some customers over others, while universities are often unable to contractually protect themselves against the costs of service migration and data portability. Third and last, it can be argued that the effects of market concentrations and technology-and-vendor lock-ins, in particular the potential deterioration of service levels and lack of innovation, could be disruptive to scientific research and subsequently hinder universities’ mission to contribute to scientific advancement.

Dutch universities locked-in with Microsoft?

In the Netherlands, most, if not all, universities use the Microsoft Office suite,²³¹ a set of applications providing seamlessly digitally connected products and services including e-mail (Outlook), video-conferencing (Teams) and online collaboration tools (SharePoint Online). The question is whether this monoculture has become

²²⁰ ACM Market Study Cloud Services 2022.

²²¹ This may be different, however, for smaller organisations that are generally more flexible and agile to switch to other providers. See Bundesministerium für Wirtschaft und Energie 2021, p. 46.

²²² ACM Market Study Cloud Services 2022, p. 5.

²²³ Or just because of unwillingness of the provider to support the transfer of data to a different service. See e.g., University of California, UCACC and UCOLASC, 2019, p. 7-8, describing the situation where the University of California requested the data and metadata faculty members had provided to a small software company (notably, not a cloud service provider) which had later been acquired by Elsevier, and where Elsevier refused to provide the data when the University requested them.

²²⁴ ACM Market Study Cloud Services 2022, p. 64.

²²⁵ Ibid.

²²⁶ Ibid. p. 6, 60, 63-64, 73.

²²⁷ Schumann and Simantke (Investigate Europe) 2017 about the vulnerability of Microsoft programmes; see also ACCSS initiative of Dutch cybersecurity professors, Open Letter 2021.

²²⁸ In 2020, multiple integrated Google-services were unavailable for few hours due to a technical malfunction, preventing many business and private users to use Google Workspace. See P. Sabel, ‘Google-storing komt hard aan’, *de Volkskrant* 15 December 2020.

²²⁹ In 2019, the Dutch Maastricht University was hit by a cyber-attack, leaving students and staff unable to access their e-mail, scientific data, the library, Blackboard and other digital services for a few days, see <<https://nos.nl/artikel/2316120-universiteit-maastricht-kampt-met-ransomware-aanval>>.

²³⁰ Ruggieri 2022, p. 20. In other words, digital technology providers have their hands on the “digital killswitch”, see Másson Maack 2017 about Microsoft, <<https://thenextweb.com/news/europe-is-living-under-microsofts-digital-killswitch>>.

²³¹ Maex and Bakker 2022, p. 42.

problematic and whether the collective use of Microsoft Office requires re-assessment. Part of the answer to that question lies in the possibility for universities to switch to alternative providers if desired. The problem with Microsoft's software, however, is that its source codes are kept confidential (proprietary software), preventing potential competitors from correctly displaying information created with Microsoft programmes²³² and thus complicating switching.²³³ Universities may also incur high training costs to teach employees how to operate new systems.²³⁴ Nevertheless, practice shows that it is not impossible for (public) organisations to migrate to other commercial providers of digital office applications or even to open source programmes. The French gendarmerie and the Italian Ministry of Defence, for example, both migrated in the 2000s and 2010s from Microsoft to free and open source software, i.e., LibreOffice (both)²³⁵ and Linux (gendarmerie).²³⁶ In 2020, the city of Munich announced its decision to shift to open source software, after it had already decided to migrate from Microsoft to open source in 2006²³⁷ and back to Microsoft in 2017.²³⁸ The back-and-forth of Munich, the pressure that is apparently still felt by the French gendarmerie to return to Microsoft,²³⁹ and the fact that to this day, many governments in Europe still run on Microsoft software, suggests that it would not be easy for universities to put an end to the use of Microsoft.

The role of competition law enforcement

In 2019, the Dutch competition authority ACM cleared the acquisition of a distributor of educational materials and owner of the digital learning management system 'Magister' (Iddink Group) – used in many high schools in the Netherlands – by a dominant publisher of (digital) educational materials (Sanoma), subject to certain conditions.²⁴⁰ One of the regulatory authority's concerns from a competition perspective was that the acquisition would put Sanoma in a position of power to prevent other publishers from offering their digital educational materials through Magister. To reduce this risk, the Dutch competition authority demanded that Sanoma would ensure that other educational publishers were granted access to Magister under "fair, reasonable and non-discriminatory" (FRAND) conditions, as well as to the data residing in Magister so that these publishers can improve their products and services in the same way as Sanoma. With this condition, the competition authority specifically aimed to protect the level playing field for educational publishers in the digital space.

3.2.2 Bundling of read-and-publish services and data analytics services

What could arguably be considered as a special lock-in-strategy specifically aimed at universities, is the practice of 'digital product and service bundling' by academic publishers. Over the past years, major scholarly publishers such as Elsevier, Springer, Pearson and Wiley have adapted their business models and transitioned from being traditional publishing companies to full-fledged data analytics corporations.²⁴¹ Not only were the publishers able to use their extensive content assets to develop current research information management systems and digital decision-making support tools, they also managed to expand their product and service portfolios by purchasing²⁴² existing scholarly infrastructures and other data analytics companies.

²³² Schumann and Simantke 2017 (Investigate Europe).

²³³ Because, if one or a few universities would decide to switch providers, they would probably not be able to collaborate/interact with the other organisations anymore that still use Microsoft Office Suite ('network effect').

²³⁴ Måsson Maack 2017.

²³⁵ Schumann and Simantke 2017 (Investigate Europe).

²³⁶ Mastrodonato 2016, <<https://www.zdnet.com/article/from-microsoft-to-libreoffice-how-italys-military-is-starting-its-march-to-open-source/>>.

²³⁷ Due to compatibility issues, the city had to run the open source system and Microsoft system side by side.

²³⁸ Schaer 2020, <<https://www.zdnet.com/article/linux-not-windows-why-munich-is-shifting-back-from-microsoft-to-open-source-again/>>.and references.

²³⁹ Schumann and Simantke 2017 (Investigate Europe).

²⁴⁰ ACM Besluit 2019. The clearance was later assessed by both a district court (ECLI:NL:RBROT:2021:1766) and a specialised supreme administrative court (ECLI:NL:CBB:2022:411), but the conditions attached to the acquisition were not altered.

²⁴¹ Aspesi et al 2019a (SPARC Landscape Analysis), p. 6-7; for Pearson specifically, see Williamson 2021, p. 62-64.

²⁴² E.g., Elsevier acquired Mendeley (a company providing academic reference management) in 2013, SSRN (preprint repository) in 2016 and Bepress (institutional repository) in 2017. See University of California, UCACC and UCOLASC 2019, p. 2. See also Aspesi and Brand 2020, p. 575.

As a result of these developments and acquisitions, Elsevier, for instance, now runs multiple companies offering services relevant to the research workflow including Mendeley (reference management software), ScienceDirect and SSRN (publications databases), Pure (Research Information Management System), Scopus (academic search tool) and SciVal (bibliometrics tool). Finding themselves in the luxurious position to offer “bundled” contractual arrangements to universities in which traditional access-to-content and publishing services are conditioned upon the purchase of data analytics services with price breaks, the publishers have a big advantage over stand-alone vendors of academic analytics products.²⁴³ Indeed, switching to alternative data analytics services does not seem attractive if that means universities would lose access to the academic publishing products. Such bundles of services are expected to only grow larger and larger until they eventually cover the entire research workflow (“platform package”²⁴⁴), which would further marginalise competitors in each market segment and increase the costs for switching.²⁴⁵

The Dutch consortia/Elsevier Agreement

In 2020, the Dutch Universities (including the University Medical Centres), Dutch Universities of Applied Science, the Royal Netherlands Academy of Arts and Sciences (KNAW) and the Dutch Research Council (NWO)²⁴⁶ concluded a multi-year agreement with scholarly publisher Elsevier on reading services, publishing services and the joint development of services for research intelligence and scholarly communication.²⁴⁷ The traditional “read-and-publish”-part of the contract provides that the institutions can access and use Elsevier’s extensive collection(s) of journals²⁴⁸ and that academic authors have the right to publish an unlimited number of open access journal articles per year in Elsevier Gold Open Access and Hybrid Journals (if accepted for publication, of course).²⁴⁹ In addition, parties agreed to collaborate on pilots aimed at creating “professional services for Research Intelligence and Workflow”. Examples of pilot services mentioned in the agreement are: services that aggregate and deduplicate current research information systems (CRISs) into a single Pure Community module; services that link research data from various institutes into a single Dutch knowledge base; services that link funding information to research outputs; and services for the better recognition on academic performance.²⁵⁰ In 2019, when the contract negotiations were still ongoing, academics were deeply worried that Dutch universities would lock themselves into Elsevier’s digital infrastructures by agreeing to full cooperation in research intelligence projects in exchange for open access publishing.²⁵¹ The Dutch negotiators managed to mitigate this risk by proposing a set of principles²⁵² governing the pilots and securing institutional discretion on the use of services, interoperability, transparency, access to research data and metadata, and data portability.²⁵³ Although Elsevier’s commitment to these principles has been applauded, concerns about its power over Dutch research infrastructures and metadata about research have not been resolved fully.²⁵⁴

²⁴³ Aspesi and Brand 2020, p. 574-575. See for example the Open Science Platform Products and Services Agreement of 15 May 2020 as concluded between Elsevier and Dutch higher education institutions represented by SURF, in which Elsevier granted the institutions access to subscription journals and open access journal services in exchange for the wide adoption by the institutions of “professional services” related to research metadata to be made available by Elsevier on a pilot basis, such as services that link research outputs to grants and funders, and services that link research data kept in subject or domain specific repositories into a single Dutch knowledge base (see Schedule 5 of the Agreement’).

²⁴⁴ SPARC 2022 (Interfolio Acquisition Report).

²⁴⁵ Ibid.

²⁴⁶ Represented by an independent intermediary, “SURFmarket” B.V.

²⁴⁷ Open Science Platform Products and Services Agreement, Preamble, p. 1.

²⁴⁸ Open Science Platform Products and Services Agreement, Section 1.1 (p. 2) and Schedule 1 (p. 33-40).

²⁴⁹ Ibid., Schedule 4, para. 1 (p. 45).

²⁵⁰ Ibid., Schedule 5, para. 1.2 (p. 103).

²⁵¹ See e.g., De Knecht (ScienceGuide) 2019.

²⁵² These “collaboration principles” are based on a set of Guiding Principles as developed in 2020 by the VSNU Dutch Taskforce on Responsible Management of Research Information and Data which had been installed earlier that year by the Association of Dutch Universities (UvL, formerly known as VSNU). The first version of the Guiding Principles can be found here:

https://universiteitenvannederland.nl/files/documenten/Nieuwsberichten/Guiding%20Principles%20on%20Management%20of%20Research%20Information%20and%20Data_11May.pdf. The revised principles can be found here: <https://zenodo.org/record/6074944#.Y8hLchXMI2x>.

²⁵³ Open Science Platform Products and Services Agreement, Schedule 5, para. 1.2 (p. 102-103).

²⁵⁴ E.g., De Rijcke 2020; SPARC 2020 (Dutch Consortia/Elsevier Contract).

3.2.3 Commercial influence on research, education and university decision-making

Another concern frequently raised by university representatives – and one very unique to the university sector – is the risk that commercial digital technology providers on which universities depend exert influence on academic research and education as well as university decision-making processes, thereby undermining individual academic freedom and institutional autonomy. This risk is sometimes referred to as a “cognitive lock-in”.²⁵⁵

Over time, commercial suppliers have become a driving force in the design of public universities’ research and teaching environments,²⁵⁶ while universities and academics are typically not involved in any of the design choices.²⁵⁷ Control over the design of digital tools, however, naturally comes with control – or at least influence – over users’ practices.²⁵⁸ University representatives therefore argue that when academic digital tools and services are designed and shaped by external commercial parties, both in terms of affordances and constraints, these parties can to a certain extent govern (explicitly or implicitly) how researchers, teachers and students behave. This, in turn, affects how scientific knowledge is accessed, produced and transmitted.²⁵⁹ Considering that commercial digital technology providers have agendas that often focus on economic expansion and profit-making, it is safe to assume that their tools are not necessarily informed by academic values but rather by their own commercial objectives and values.²⁶⁰

The question that arises in this regard is at which point commercial influence on research and teaching becomes problematic from the perspective of individual academic freedom, institutional autonomy and scientific advancement more generally. This is not a black and white issue, but more of a sliding scale. At the one end of the continuum, there is the technology provider who gives users abundant freedom to determine how to use its tools, for instance by providing various options to view and display content. On the other end of the spectrum, there is the technology provider who decides to shut down its service because it does not approve the objectives a university or academic is using its tool for (see below). All situations in between these two extremes have to be assessed on a case-by-case basis in order to determine whether the commercial intervention in question violates academic values.

Zoom shuts down university webinar

The shut-down scenario really occurred in 2020, when the popular video-conferencing tool Zoom unilaterally ended a webinar hosted by the NYU chapter of the American Association of University Professors (AAUP) on – ironically – censorship, for the reason that the online presence of a controversial Palestinian activist breached Zoom’s terms of service.²⁶¹

Besides research and teaching, commercial digital technologies are also widely used in administrative university processes. As providers of (much welcomed) tools for, e.g., the evaluation of productivity and performance of staff, students and institutions themselves,²⁶² commercial companies are in the position to technically define what constitutes “valuable performance” in a university context.²⁶³ Considering that the

²⁵⁵ UvA, ‘Aanzet roadmap Q1 2022: Digitale Soevereiniteit’ [internal document].

²⁵⁶ LERU Data Statement 2021.

²⁵⁷ Maex et al 2019.

²⁵⁸ Gürses 2020 (Part 1 and Part 3).

²⁵⁹ LERU Data Statement 2021; Maex et al 2019; Maex, 2021; UVL/VNSU 2021, p. 1 (about influence on the teaching process, contents of education and students’ learning activities); Williamson 2016, p. 138 (“The new managers of the virtual world of educational data are the technical, statistical, methodological and graphical experts”); Williamson and Hogan 2021, p. 56-57 (about learning management systems); Gürses 2020 (Part 1 and Part 3).

²⁶⁰ Maex, 2021, p. 3; Gürses 2020 (Part 1 and Part 3).

²⁶¹ NYU AAUP Statement 23 October 2020, <<https://www.nyu-aaup.org/statement-on-zoom-censorship/>>; see also Leland 2021.

²⁶² For example, Elsevier SciVal, which delivers research performance metrics, <<https://www.elsevier.com/solutions/scival>>. See also Elsevier Analytical Services, which provides reports on research performance more broadly, <<https://www.elsevier.com/solutions/analytical-services>>.

²⁶³ Williamson 2021, p. 61-62.

insights generated by these tools are increasingly used to underpin university decisions on for example resource allocation, investments in emerging relevant research fields, career advancement (promotion, tenure) and student assessment,²⁶⁴ it is the commercial designer of the tool who can indirectly determine how organisational behaviour is shaped.

Again, the question here is at which point commercial influence on administrative university processes becomes problematic. And again, this is a sliding scale. At one end of the continuum, there is the human decision-maker who takes the insights generated by digital productivity tools into account as a subfactor in the overall decision-making process. At the other end of the spectrum, there is the human decision-maker who gives disproportionate weight to productivity tools, for example due to a lack of money or time to make his own evaluation. Relying fully on standardised and often opaque algorithms, however, could lead to decisions that conflict with institutional policies and values.²⁶⁵ Universities should therefore prevent that their operations are fully governed by technology and ensure that commercial companies do not become de facto policy centres for higher education.²⁶⁶

Commercial influence on research (evaluation): the case of Google Scholar

An example of a commercial digital tool influencing academics' behaviour is the popular academic search engine offered by Alphabet Inc.: Google Scholar. Google Scholar indexes large amounts of academic literature – including so-called “grey literature”²⁶⁷ such as blogs, newspaper articles and preprints – by and for researchers. Researchers can insert queries in the search bar, on the basis of which the search engine displays a list of the most relevant literature matching the query. However, how Google Scholar's algorithms exactly determine whether a source is ‘relevant’ to a user remains unclear. Researchers have limited options to customise search results, as Google Scholar only allows the user to filter results based on date range and specific author or journal, but not on for example discipline, document type, jurisdiction or other criteria. Thus, researchers' access to digitised academic information is to some extent determined by commercially-defined, unclear and unchallengeable notions of relevance rather than researchers' own standards.²⁶⁸ Importantly, commercial influence on research also stretches out to the way research is evaluated. As explained in Chapter 2, individual academic freedom has an evaluative dimension, meaning that academics should be evaluated by their peers and not by public authorities or private actors. This ideal is increasingly challenged by the growing centrality of Google Scholar's system of evaluative bibliometrics and citation counting. Google Scholar Citations displays scholar profiles which include, among other things, researchers' h-index and i-10 index values. The h-index is an indicator of a scholar's impact and is calculated based on the number of papers published by the researcher and the number of citations referring to those papers. The number of citations informing the h-index are retrieved from Google Scholar's system for citation counting across the index database. The problem with this method of “evaluation” – which is becoming more and more important in daily academic practice, for instance in job applications, the selection of papers to read and/or prescribe to students, and supposedly even in promotion decisions – is that the scale of Google Scholar's index and the mechanism for extracting citations are not transparent and non-accountable. The opacity of the system leads to the undesirable situation where academics and universities do not seem to (fully) understand how they evaluate themselves (if this rigid quantitative approach constitutes an evaluation after all) which is arguably at odds with academic freedom.²⁶⁹

3.3 Claims relating to data

²⁶⁴ Aspesi et al 2019a (SPARC Landscape Analysis) p. 5, 16-17; Aspesi and Brand 2020, p. 575.

²⁶⁵ Aspesi et al 2019a (SPARC Landscape Analysis), p. 32.

²⁶⁶ Williamson and Hogan 2021, p. 57.

²⁶⁷ Goldenfein and Griffin 2022, p. 12.

²⁶⁸ *Ibid.*, p. 7, 13-14. Empirical work suggests that the relevance is based on the number of times an article is referenced by other documents in the scholarly index (citation count), but this has not been confirmed by Alphabet; Goldenfein and Griffin 2022, p. 13.

²⁶⁹ Goldenfein and Griffin 2022, p. 10-11; Goldenfein et al 2019.

As discussed in Chapter 1, commercial digital technology providers often aim to “capture” the value of data uploaded to and generated by users of their digital infrastructures. Meanwhile, providers of digital infrastructures tend to keep their own data secret, thereby closing off avenues for certain data-driven research projects. Relatedly, while research performing organisations are legally obliged to make publicly funded research data publicly available for re-use (see Chapter 4), the private sector does not – subject to a few exceptions – bear such legal obligations of openness. This can hamper universities’ and academics’ ability to carry out public-interest-driven scientific research.

3.3.1 Large-scale (meta)data collection and exploitation

An important generic concern raised by university representatives is that many, if not all, digital technology providers collect large volumes of behavioural data generated by the end-users of their services and potentially infringe on end-users’ privacy and protection of personal data. Academic researchers are considered an interesting target group, as information on research activity – “research intelligence” – can inform research policy, rendering the data competitively valuable assets in the hands of companies that can be sold back to universities to assist institutional decision-making processes.²⁷⁰ Data on researchers’ search inputs, time spent engaging with information sources, dates and avenues of publications, numbers of citations and so on are collected and stored via technical tracking instruments such as page visit trackers, third-party plug-ins and the harvesting of bidstream data.²⁷¹ These data may contain personal data – that is, if researchers are identifiable, based for example on their device information – and are often collected without the researchers’ knowledge, let alone their explicit consent. Moreover, it is not guaranteed that the data are in safe hands with commercial companies. Not only have commercial digital technology providers sold data to third parties in the past,²⁷² the companies may also be subject to foreign legislation such as the US CLOUD Act that allows foreign governments under certain circumstances to access the data held by these companies.²⁷³

Besides general privacy and data protection concerns, data tracking also raises specific concerns from the perspective of academic freedom. As explained in Chapter 2, it is necessary for the effective exercise of academic freedom that researchers can conduct research activities free from any kind of surveillance by the State or other actors.²⁷⁴ When researchers feel watched in the digital domain while conducting their research, they may decide to practice self-censorship, for instance because they do not want to be perceived as controversial (chilling effect).²⁷⁵

Research data tracking through Pure

Elsevier’s research information management system ‘Pure’ serves as a platform for researchers to enter and manage data about research and other related content. The system can be used to monitor research progress, showcase publications, generate reports (statistics) and plan and evaluate research activities. Through Pure, Elsevier has access to millions of researcher profiles, citation and publication numbers and behavioural data generated by researchers using Pure, which makes the system a gold mine for the development of business intelligence software to support evidence-led decision-making within universities.²⁷⁶

²⁷⁰ DFG Briefing Paper 2021, p. 6; see also Schaafsma and Van der Meer 2022, who emphasise that the data come from the universities’ own pockets (or as the Dutch say goes: “a cigar from one’s own box”).

²⁷¹ DFG Briefing Paper 2021, p. 10-11.

²⁷² In 2021, LexisNexis (part of Elsevier) sold extensive personal information it had collected to US federal immigration authorities, see CBS News 2022, <<https://www.cbsnews.com/news/lexisnexis-lawsuit-collected-sold-personal-data-immigration-advocates-allege/>>.

²⁷³ ACCSS Open Letter 2021, signed by 19 Dutch cybersecurity professors.

²⁷⁴ ARTICLE 19 Policy Brief 2017 on privacy and freedom of expression, p. 4; see also Dab, in: LERU New Year’s Debate 2022 (01:26:55 and further).

²⁷⁵ Tanczer et al 2020, p. 4.

²⁷⁶ Schaafsma and Van der Meer 2021.

The commercial extraction and exploitation of data arguably also has a broader impact, beyond the individual level, on science as a whole. Various university representatives have expressed the fear that information about research generated within commercial digital infrastructures gets “locked up in private corporate silos”,²⁷⁷ as a result of which “public goods [are turned] into private assets”²⁷⁸ and “the knowledge society [may become] predominantly privatised.”²⁷⁹ The concentration of research intelligence in the hands of private entities conflicts with the idea of open science, and, ultimately, scientific advancement.

Privatisation of metadata on research

Metadata about scholarly output – such as the publication’s title, the author(s), the authors’ affiliations, the publication’s keywords, the abstract and the reference list – are commonly stored in commercial citation bases such as Scopus and Web of Science. Admittedly, the metadata are usually also submitted to institutional current research information systems (CRISs), but the data in those systems are often fragmented and/or lack quality. Moreover, the data entered in one CRIS are not automatically shared with other CRISs. Obtaining overviews, evaluations and assessments of research therefore largely depends on commercial research intelligence services which are integrated with the commercial citation databases. In order to address the information asymmetry between universities and commercial entities, the Association of Dutch Universities (UNI) has proposed the creation of an “Open Knowledge Base” in which all metadata, metrics and analyses from all CRISs are made openly available for everyone to benefit from.²⁸⁰

3.3.2 Limited access to data for research purposes

Whereas commercial digital technology providers are able to access scientific research and open research data, researchers do often not know much about the providers that accumulate enormous amounts of valuable data on social, economic, political and cultural activities, processes and phenomena. The problem is that these companies are generally not willing to share such data with outsiders. Empirical research shows that academic researchers sometimes experience difficulties in accessing data residing in digital infrastructures managed by the private sector, which prevents them from studying and observing parts of the digital world around us.²⁸¹ This is arguably detrimental to their public-interest mission to contribute to scientific advancement. For a more detailed overview of the obstacles academic researchers may run into when trying to access externally-held data, reference is made to the research report produced by the Institute for Information Law on the topic of data access for research purposes (**Part II**).²⁸² The report also shows that the legal landscape for researchers’ data access is highly fragmented and does rarely grant researchers strong actionable claims to third-party data.²⁸³

3.3.3 Instrumentalisation of publicly-funded research data for commercial gain

Finally, there are concerns that the interfaces between open science policy (see Chapter 4) and private sector business models are not well-constructed. Private actors may enlist public research performing organisations to carry out research and, in keeping with the latter’s legal obligations, have them make the respective research data accessible and available for re-use. The fact that not-for-profit scientific research benefits from exceptions under EU copyright law and data protection law renders universities and public research institutions more attractive for industry-sponsored (preparatory) research which can subsequently be used

²⁷⁷ Sellar and Hogan 2019, p. 1.

²⁷⁸ Ibid., p. 2.

²⁷⁹ DFG Briefing Paper 2021, p.7; LERU Data Statement 2021.

²⁸⁰ See <https://www.universiteitenvannederland.nl/nl_NL/os_onderzoekinformatiesystemen-open-knowlegde-base.html> and the feasibility study into the Open Knowledge Base by Kemman and Te Velde 2021.

²⁸¹ See e.g., references in: Ausloos and Veale 2020, p. 136–57; Ausloos, Leerssen, and Ten Thije 2020; and Rieder and Hofmann 2020.

²⁸² Institute for Information Law 2023b.

²⁸³ Except for Article 40 of the Digital Service Act for online platform data, subject to conditions.

as an input for commercial products. In the field of generative AI training, for instance, private actors collaborate with public research institutions to generate open research data and (pre-)train AI models for subsequent commercial use, thereby avoiding accountability and liability for data acquisition.²⁸⁴

While EU law, and in particular the Open Data Directive, currently requires public research performing organisations to increasingly invest in the management and open sharing of research data, the private sector does not – or at least not to the same degree – bear such legal obligations of openness to facilitate scientific research. Admittedly, the upcoming Data Act aims to stimulate the sharing of private sector data but does not go as far as to oblige commercial actors to contribute to the open data ecosystem. A data ecosystem where the costly production of open research data is placed on public-value oriented research institutions²⁸⁵ and where private actors can turn these open data into proprietary knowledge and commercial business models, produces an unsustainable dynamic that collectivises the cost of open science for private gains, which is highly problematic from the perspective of scientific advancement to the benefit of all.

²⁸⁴ Quintais 2023; Baio (WAXY) 2022.

²⁸⁵ Kitchin 2014.

3.4 Universities' agency to address digital sovereignty claims and its limits

It could be argued that universities' digital sovereignty claims are partly the result of their own institutional decision-making. Until recently, universities mainly focused on solving short-term operational problems rather than their sustainability and independence.²⁸⁶ Like any organisation, universities find it important that the digital services they procure are qualitatively good, user-friendly, efficient and reasonably priced.²⁸⁷ However, as discussed above, digital service procurement can put other critical values at risk.²⁸⁸ In particular during the COVID-19 pandemic, universities quickly adopted controversial digital tools such as real-time exam fraud detection software and (initially) non-privacy-friendly video conferencing tools to support the continuity of education and facilitate remote working.²⁸⁹ Although those decisions were more than sensible given the abnormal circumstances of the time, it was only later that universities started to question the integrity, data privacy, and security of certain digital services and the potential repercussions for the fundamental rights of their researchers, teachers and students.²⁹⁰ Just recently, universities started to evaluate the dangers associated with commercial outsourcing and growing dependencies to their institutional autonomy and public-interest mission. There has been a collective realisation that universities urgently need a long-term strategic vision to address the risks of the digital transformation, a realisation that is being translated into claims for digital sovereignty.

In response to this realisation, new strategies have emerged within the university sector. Universities aim to leverage the potential of the digital transformation, while at the same time shaping digitalisation processes in ways so as to protect and promote public values. For example, two Dutch non-profit organisations within the educational ICT sector (SURF and Kennisnet²⁹¹) together developed a 'Value Compass'²⁹² to structure the digital transformation in (higher) education and research. The compass prioritizes three core values in the design, procurement and use of innovative technologies: justice, humanity and autonomy. Each of these values, in turn, encompasses sub values such as equality, social connection, freedom and independence. For each new digital possibility – whether it involves the procurement of a commercial digital tool, the use of an open source or self-hosted tool, or a public-private research collaboration with a technology company – these values must be explicitly balanced against functional, financial and efficiency benefits. In parallel, the University of Amsterdam developed a five pronged-approach to tackle digital sovereignty that includes the following steps: (1) raising awareness on the issue of digital sovereignty; (2) performing research to get a grip on the issues; (3) supporting the development of public digital infrastructures; (4) defining procurement mechanisms to guard digital sovereignty; and (5) using digital laws and lobby to amend legislation in order to protect the digital sovereignty of universities.²⁹³ This report has been commissioned as part of step (2).

Lessons can also be learnt from other actors and sectors. In an **expert memorandum** commissioned by the Institute for Information Law, Arnold Roosendaal – privacy expert and director of the Dutch consultancy firm Privacy Company – explains how the General Data Protection Regulation may be utilised as a means to protect universities' data and digital sovereignty.²⁹⁴ Drawing from Privacy

²⁸⁶ Hoepman 2021; Schaafsma and Van der Meer 2021; see also ACCSS Open Letter 2021, signed by 19 Dutch cybersecurity professors.

²⁸⁷ According to a board member of the University of Amsterdam, SURF Summit 2022. See also Bok et al (VSNU) 2021, p. 5.

²⁸⁸ See also Bok et al (VSNU) 2021, p. 1.

²⁸⁹ In literature, the outbreak of the COVID-19 pandemic and the subsequent decisions and actions taken by universities have been referred to in literature as a "let's first get things done"-moment", Gürses 2020 (Part 1), referring to Aouragh et al 2015.

²⁹⁰ Williamson and Hogan 2021, p. 61-62.

²⁹¹ SURF is collaborative organisation for ICT in Dutch higher education and research, see <<https://www.surf.nl/en>>; Kennisnet is a public organisation funded by the Ministry of Education, Culture and Science which provides a national ICT-infrastructure for primary, secondary and vocational education and training, see <<https://www.kennisnet.nl/about-us/>>.

²⁹² SURF is collaborative organisation for ICT in Dutch higher education and research, see <<https://www.surf.nl/en>>; Kennisnet is a public organisation funded by the Ministry of Education, Culture and Science which provides a national ICT-infrastructure for primary, secondary and vocational education and training, see <<https://www.kennisnet.nl/about-us/>>.

²⁹³ UvA, 'Aanzet roadmap Q1 2022: Digitale Soevereiniteit' [internal document].

²⁹⁴ A. Roosendaal, 'The GDPR as a means to protect digital sovereignty of universities', 2023.

Company's vast experience with Data Protection Impact Assessments (DPIAs), particularly those performed in relation to Google Workspace (G Suite),²⁹⁵ Microsoft Office,²⁹⁶ Zoom²⁹⁷ and Amazon Web Services,²⁹⁸ Roosendaal argues that a DPIA can be a powerful instrument to regain control over the data processed by commercial digital technology providers. As practice has shown, a public document with legal-technical findings on non-compliance with the GDPR can be used to force service providers to make the necessary changes, thus enhancing the position of buying organisations vis-à-vis powerful technology companies. In other words, a DPIA can serve as a 'sword' for universities to renegotiate contracts with commercial digital technology providers and regain independence.

Yet, there are limits as to what universities can do, individually or collectively, to address claims for digital sovereignty. For certain complex, meta-level problems such as highly concentrated market structures and anticompetitive practices, the average approach to university procurement may simply not yield adequate solutions. It is well documented that certain digital markets have been prone to technology-and-vendor lock-ins, bundling of digital services, suboptimal interoperability or data extractivism, all of which can be very difficult to overcome for an average business client. Typically, the freedom of contract succumbs to the sheer bargaining power of large digital platforms which hardhandedly force their way with the help of ostensibly non-negotiable standard terms of service. This is further compounded by information asymmetries which distort the ability of clients to negotiate contracts that are fully GDPR-compliant.

In conclusion, in some areas, legal and/or policy intervention is needed to complement universities' own measures to address digital sovereignty claims. The next chapter therefore focuses on what EU law and digital policy already do, and also what they fail to do, in regard to universities' and academics' digital sovereignty.

²⁹⁵ See <<https://www.privacycompany.eu/blogpost-en/privacy-assessment-google-workspace-g-suite-enterprise-dutch-government-consults-dutch-data-protection-authority-on-high-privacy-risks>>.

²⁹⁶ See <<https://www.privacycompany.eu/blogpost-en/new-dpia-for-the-dutch-government-and-universities-on-microsoft-teams-onedrive-and-sharepoint-online>>.

²⁹⁷ See <<https://www.privacycompany.eu/blogpost-en/new-dpia-for-surf-and-dutch-government-on-zoom-all-high-risks-solved>>.

²⁹⁸ See <<https://www.privacycompany.eu/blogpost-en/new-dpia-and-dtia-on-aws-for-the-dutch-government-all-high-risks-solved>>.

4. Impact of EU law and policy on digital sovereignty in the university context

Having established an account of digital sovereignty claims that can be made in the university context, this report now turns to the role of EU law and policy. On the one hand, law and policy can be used as tools to facilitate universities' quest for digital sovereignty and strengthen it. On the other hand, law and policy may fail to give due recognition to research-performing organisations such as universities and create legal obligations that are not well-attuned or even burdensome to scientific research. This Chapter explores to what extent the current and emerging EU regulatory environment for the digital era provides safeguards for universities' and academics' digital sovereignty – or at least 'hooks' to which digital sovereignty-promoting strategies can be attached – and to what extent universities' (digital) interests should receive better recognition from lawmakers.

4.1 EU policies for the digital age

The EU has taken a proactive role in shaping the digital transformation through its policies and legislation. The EU's Open Science policy and the Open Data Directive specifically aim to promote scientific research in the digital age. Other EU digital law-making, however, rather has *indirect* effects on universities, academics and their scientific activities.

The **EU's Open Science Policy** focuses on spreading knowledge and data through digital and collaborative technologies.²⁹⁹ It is rooted in the Union's foundational objective to strengthen its scientific and technological bases by establishing a "European Research Area" (ERA) in which researchers, scientific knowledge and technology can circulate freely.³⁰⁰ The Open Data Directive has translated some of the principles of the EU's Open Science Policy into law.³⁰¹ This recast of the former Public Sector Information (PSI) Directive seeks to facilitate the re-use of public data for the benefit of the European economy and society. First launched in the year 2000, the ERA strategy was recently updated to make it more impactful.³⁰² Corresponding with the new strategy, the Council of the European Union defined in its "Pact for Research and Innovation"³⁰³ four priority areas for joint action in support of the ERA. The "European Research Area Policy Agenda of 2022-2024", in turn, lays down several implementing actions for these priority areas.³⁰⁴ One of the actions listed in the Policy Agenda, and an important pillar of the EU's Open Science policy, is the development of a European Open Science Cloud (EOSC).³⁰⁵

European Open Science Cloud (EOSC)

²⁹⁹ Website of the European Commission, 'Strategy on research and innovation > Strategy 2020-2024 > Our digital future > Open Science', <https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/our-digital-future/open-science_en>.

³⁰⁰ Article 179(1) of the Treaty on the Functioning of the European Union.

³⁰¹ Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), recitals 4, 27.

³⁰² Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a New Era for Research and Innovation, COM(2020) 628 final; endorsed by the Council conclusions on the New European Research Area, 1 December 2020, 13567/20.

³⁰³ Council Recommendation (EU) 2021/2122 of 26 November 2021 on a Pact for Research and Innovation in Europe.

³⁰⁴ European Commission, 'European Research Policy Agenda – Overview of actions for the period 2022-2024', November 2021.

³⁰⁵ *Ibid.*, p. 4-5; see also the European Commission Open Science' webpage at: <https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/our-digital-future/open-science_en>. For more detailed information on the EU's Open Science Policy, see European Commission, Mendez and Lawrence 2020.

The EOSC is a long-term and joint initiative of the Commission and the European research community to develop a federated virtual environment to store, share, process and re-use digital research objects, such as publications, data and software. One of project’s goals is to bring together existing and future research infrastructures that are currently scattered across disciplines and Member States around a shared core, and ensure that domain-specific, national, regional and institutional research repositories are connected within a single pan-European governance structure.³⁰⁶ The EOSC ‘hub’ will be implemented in the coming years through a number of projects.³⁰⁷ It must moreover become a ‘data space’ that facilitates access by interested parties (not just research institutions) to a wide range of multi-disciplinary research-related resources, such as datasets, computational power, data storage, data analysis programmes, identity and access management services, training and support materials, and more.³⁰⁸ Organisations can register their resources into a catalogue which is made publicly available to prospective users via the EOSC Marketplace.³⁰⁹

Importantly, the pursuit of open science is only one aspect of the EU’s broader digital strategy to secure a “better digital future for everyone”.³¹⁰ To this end, the European Commission has been implementing various strategies covering multiple policy domains, such as data,³¹¹ digital services and online platforms,³¹² cybersecurity,³¹³ and Artificial Intelligence,³¹⁴ among others. The already complex web of EU data and digital legislation is expected to only grow in the future, especially since the European Commission has announced an “intensification” of the actions defined in earlier strategies.³¹⁵

Although this (primarily economic) regulation does not necessarily target science in particular, it does create legal obligations of compliance and in some instances also legal privileges for scientific research. This Chapter offers an overview of selected legislative instruments under the EU’s digital policy agenda and assesses their impact on universities and academics in terms of rights/entitlements and obligations/burdens. The legislative instruments that are deemed of particular importance to universities and scientific research are listed in the table below.

| Domain | Data protection and data governance | Digital services | Intellectual property | Artificial Intelligence |
|--------------------|---|----------------------------------|--|--------------------------------|
| Legislation | General Data Protection Regulation (2016/679) | Digital Services Act (2022/2065) | Copyright in the Digital Single Market Directive (2019/790), read in | Proposed AI-Act |
| | Free Flow of Non-Personal Data Regulation (2018/1807) | Digital Markets Act (2022/1925) | | |

³⁰⁶ European Commission, COM(2016) 178 final, p. 7.

³⁰⁷ EOSC-hub, for example, sets up the federation and management system of EOSC; OpenAIRE provides guidelines and training on open science. For more EOSC Projects, see <<https://eosc-portal.eu/about/eosc-projects>>. See also Horizon Europe Work Programme 2023-2024 – 3. Research Infrastructures, C(2023) 2178, 31 March 2023, p. 36-77.

³⁰⁸ European Commission, ‘EOSC: the Transverse European Data Space for Science, Research and Innovation’, 2022: <<https://op.europa.eu/nl/publication-detail/-/publication/61134f17-7f50-11ed-9887-01aa75ed71a1>>.

³⁰⁹ See <<https://eosc-portal.eu/for-providers>>.

³¹⁰ European Commission, Communication ‘Shaping Europe’s digital future’, COM(2020) 67 final, 19 February 2020. See also European Parliament Digital Agenda Factsheet.

³¹¹ See e.g., the European Commission Communication on a European strategy for data, COM(2020) 66 final.

³¹² European Commission Digital Services Act package webpage at: <<https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>>.

³¹³ European Commission Communication on the EU’s Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final.

³¹⁴ European Commission Communication on Artificial Intelligence for Europe, COM(2018) 237 final; see also Independent High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, 8 April 2019; and White Paper on Artificial Intelligence – A European approach to excellence and trust, COM(2020) 65 final.

³¹⁵ European Commission Communication on a 2030 Digital Compass: the European way for the Digital Decade, COM(2021) 118 final.

| | | | | |
|--|---|--|--|--------------------------------------|
| | | | conjunction with the Information Society Directive (2001/29) and other intellectual property instruments | (COM(2021) 206 final) ³¹⁶ |
| | Open Data Directive (2019/1024) | | | |
| | Data Governance Act (2022/868) | | | |
| | Proposed Data Act (COM(2022) 68 final) ³¹⁷ | | | |

Table 3. A selection of legal frameworks adopted or proposed as part of the EU’s digital strategy

4.2 Rights and obligations of universities and researchers under EU digital/data law

Outside EU’s Open Science Policy, the EU’s data and digital legislation is typically not addressed to universities and academics; often they are not even recognised as relevant stakeholders. Nonetheless, universities and academics are and will be affected by EU digital legislation in a variety of ways. On the one hand, they are the beneficiaries of new **rights and legal entitlements**. On the other hand, they are the bearers of new **legal obligations** they have to comply with. This section briefly highlights the most important rights and obligations for universities and academics laid down in the selected EU instruments, in their capacities as (1) *users* of third-party digital technologies and infrastructures, including Artificial Intelligence (‘infrastructure input’); (2) *providers* of not-for profit digital infrastructures and services, such as repositories (‘infrastructure output’); (3) *users* of data for research purposes (‘data input’); and (4) *providers* of data generated or collected in the course of research activities (‘data output’).³¹⁸

4.2.1 Use of digital infrastructures and services (infrastructure input)

In their capacity as *users* of digital technologies and infrastructures, universities and academics arguably greatly benefit from provisions in EU legislation on service interoperability and data portability. Interoperability refers to the ability of two or more technical systems to exchange data interactively and mutually use the exchanged data in a way that the systems work well together.³¹⁹ Data portability refers to the ability to move, copy, transfer or transmit data from one technical system (operated by a company, data controller, service provider, and so on) to another (operated by a different company, controller or

³¹⁶ For this report, we used the text proposed by the European Parliament on 14 June 2023. Available at: <https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html>.

³¹⁷ For this report, we used the latest proposal of the Council of the European Union to which we refer as the proposed Data Act or pDA: Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act) – Mandate for negotiations with the European Parliament, 17 March 2023, 7413/23 (published 24 March 2023). Available at: <<https://www.consilium.europa.eu/en/press/press-releases/2023/03/24/data-act-member-states-agree-common-position-on-fair-access-to-and-use-of-data/>>.

³¹⁸ For a more in-depth discussion of the impact of specific instruments within the data-digital legislative framework on scientific research (i.e., not on education), reference is made to four recent expert studies commissioned by the European Commission on the Digital Services Act and Digital Markets Act, EU copyright law and the Open Data Directive, Data Governance Act and proposed Data Act. See: European Commission and Lundqvist 2022; European Commission and Angelopoulos 2022; European Commission and Senftleben 2022; and European Commission and Van Eechoud 2022.

³¹⁹ For more detailed definitions, see e.g., Article 2(29) of the Digital Markets Act; Article 2(19) of the proposed Data Act (Council version); and Gulati-Gibert and Seamans 2023.

provider).³²⁰ The easier the switching between digital services, the better the negotiation position of universities and the lesser chance of technology-and-vendor lock-ins. Data portability requirements appear in various pieces of legislation. Under the **General Data Protection Regulation**, for example, data subjects have a right to transmit, or have transmitted, their personal data to other data controllers.³²¹ The **Free Flow of Non-Personal Data Regulation** takes a self-regulatory approach to the problem of vendor lock-ins by promoting European codes of conduct to facilitate the switching between service providers and the porting of data.³²² To date, however, the self-regulatory approach does not seem to have affected market dynamics significantly, which is why the **forthcoming Data Act** opts for a regulatory approach to address vendor lock-ins (see below).³²³ Likewise, the **Digital Markets Act** contains a specific obligation addressed to providers of core platform services (online search engines, social networking sites, etc.) identified as “gatekeepers”³²⁴ to ensure free, continuous and real-time portability of data generated through business’ and end users’ activities.³²⁵ The rationale behind this requirement is that it facilitates switching, which, in turn, should lead to an increased choice for end users and be an incentive for gatekeepers to innovate.³²⁶

The aforementioned portability requirements for data controllers and gatekeepers will soon be complemented by requirements for providers of so-called ‘data processing services’³²⁷ – e.g., Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) delivery models – laid down in the proposed Data Act. Chapter VI of the proposed Regulation obliges providers of data processing services not to pose any obstacles that inhibit their users (natural persons and businesses) from terminating the service contract with a provider; concluding a new contract with an alternative provider; porting (meta)data and other digital assets³²⁸ to a different provider or to on-premise systems; or maintaining functional IT-equivalence in the environment of the different provider.³²⁹ In terms of monetary obstacles, data processing service providers must reduce and eventually abolish any charges on customers for the switching process.³³⁰ In terms of technical obstacles, covered providers are required to take measures to ensure that after switching customers enjoy functional equivalence in the use of the new service.³³¹ Data processing providers must also ensure that their services are compatible with open interoperability specifications and/or standards for interoperability.³³² In addition, Chapter VIII of the proposed Data Act imposes specific requirements facilitating the interoperability of data, data sharing mechanisms and services as well as of the common European data spaces and data processing services.³³³

Besides rights and entitlements, universities as users of digital infrastructures and services may also bear obligations. In the event that universities decide to use AI-systems as defined in the **upcoming Artificial Intelligence Act**, for instance, they must adhere to the obligations laid down therein. According to the proposed Regulation, those AI-systems used *in education* “for determining access or materially influence decisions on admission or assigning persons to educational and vocational institutions or to evaluate persons on tests as part of or as a precondition for their education or to assess the appropriate

³²⁰ For more detailed definitions, see e.g., Article 20(1) of the General Data Protection Regulation; European Commission Communication 2017, p. 46; and Gulati-Gilbert and Seamans 2023.

³²¹ Article 20 GDPR.

³²² Article 6(1)(a) FFNPD-Regulation. See the industry-developed codes of conduct for Infrastructure as a Service (IaaS) providers and for Software as a Service (SaaS) providers at SWIPO Codes of Conduct: <<https://swipo.eu/download-section/copyrighted-downloads/>>.

³²³ Explanatory Memorandum to the pDA, p. 4-5.

³²⁴ Article 2(1) jo. 2(2) jo. 3 DMA.

³²⁵ Article 6(9) jo. recital 59 DMA.

³²⁶ Recital 59 DMA.

³²⁷ Data processing services are services that enable “on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources of a centralised, distributed or highly distributed nature”, see Article 2(12) pDA.

³²⁸ This varies from applications to entire business administrations, Madiaga (European Parliamentary Research Service) 2020, p. 7.

³²⁹ Article 23 pDA.

³³⁰ Article 25 pDA.

³³¹ Article 26(1) pDA.

³³² Article 26(3) jo. Article 29(5) pDA. See also recital 79 pDA.

³³³ Article 28 and 29 pDA; these requirements can be supplemented by delegated acts, Article 28(2) pDA.

level of education for an individual and materially influence the level of education and training that individuals will receive or be able to access or to monitor and detect prohibited behaviour of students during tests”, should be considered as “high-risk AI-systems.”³³⁴ This is because such systems “may determine the educational and professional course of a person’s life and therefore affect their ability to secure their livelihood”.³³⁵ Furthermore, when these systems are “improperly designed and used”, they “can be particularly intrusive” and “may violate the right to education and training as well as the right not be discriminated against and perpetuate historical patterns of discrimination”.³³⁶ All deployers of high-risk AI-systems are subject to certain obligations, for example to employ the systems in accordance with providers’ instructions of use accompanying the systems; to implement adequate human oversight; to monitor robustness and cybersecurity measures; and most importantly, to conduct an assessment of the system’s impact in the specific context of use.³³⁷

At the same time, the proposed AI Act aims to respect the freedom of science. For this reason, both the texts of the Council and the European Parliament state – in slightly different words – that the Regulation will not apply to AI systems specifically developed for the sole purpose of *scientific research* and development.³³⁸ Such a limitation of scope would benefit research and development activities involving AI which are carried out in accordance with recognised ethical and professional standards.³³⁹ The proposed limitation of the scope of the proposed Regulation would not only benefit research performing organisations such as universities but would moreover shield providers’ product-oriented research activity before placing the product on the market.

4.2.2 Provision of digital infrastructures and services (infrastructure output)

In their capacity as *providers* of digital technologies and infrastructures – including repositories for research output, educational repositories, discussion forums, archives and libraries –, universities may have to comply with legal obligations as well. However, the exact impact of newly introduced **Digital Services Act (DSA)**, an important regulation on the provision of digital intermediary services in the Union, on universities and academics is (still) quite *unclear*. Since its proposal, there has been scholarly debate about whether the Regulation applies to universities in their capacity as providers of not-for-profit digital infrastructures and services. In contrast to the **Copyright in the Digital Single Market Directive (CDSM)**, which explicitly excluded “not-for-profit educational and scientific repositories” from the scope of its obligations imposed on content sharing services,³⁴⁰ the Digital Services Act has not excluded them.

At first sight, it seems that such services are *not* covered by the definition of “intermediary services” used in the DSA, which encompasses particular information society services, namely “mere conduit” services, “caching” services or “hosting” services.³⁴¹ Historically, information society services have been defined by the EU legislator as services that are “normally provided for remuneration (...)”.³⁴² Because university repositories and libraries are typically not provided for remuneration, they do not seem to qualify as information society services and thus to fall outside the scope of the Digital Services Act.

³³⁴ Article 6(2) jo. Annex III under no. 3 of the pAIA.

³³⁵ Recital 35 of the pAIA.

³³⁶ Ibid.

³³⁷ Article 29 and 29a pAIA.

³³⁸ See recital 2f and Article 2(5d) of the text proposed by the European Parliament on 14 June 2023, available at: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html and recital 12 and Article 2(6) of the text proposed by the Council on 25 November 2022, available at: <https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/>.

³³⁹ Recital 12(b) of the Council proposal.

³⁴⁰ Article 2(6) CDSM Directive.

³⁴¹ Article 2(1) jo. Article 3(a) and (g) jo. recital 5 DSA.

³⁴² Article 3(a) DSA with reference to Article 1(1)(b) of Directive (EU) 2015/1535.

However, older legislation using the same definition³⁴³ has stated (in recitals) that information society services “extend to services which are *not remunerated* by those who receive them (...) in so far as they *represent an economic activity*”.³⁴⁴ Whether this economic-activity criterion is also relevant under the Digital Services Act is uncertain.³⁴⁵ In practice, most services offered by public universities are closely connected to the exercise of their public function and can therefore not be considered as economic activities.³⁴⁶ Following this line of reasoning, the Digital Services Act seems only of marginal relevance to university repositories and libraries. *If*, however, relevant “hosting” services can be considered an economic activity, for example when a repository is set up as a corporation or a public-private partnership, they could fall within the scope of the Digital Services Act, which means that universities must comply with the relevant (transparency and due diligence) obligations contained therein.³⁴⁷ Nevertheless, “hosting” providers are to a certain extent shielded by the general liability limitation in Article 6 of the Digital Services Act. Yet also this limitation is not infinite and a duty to “expeditiously to remove or to disable access” arises with “actual knowledge of illegal activity or illegal content”.³⁴⁸

4.2.3 Use of data for research purposes (data input)

Turning to the dimension of data, universities and academic researchers in their capacity as *users* of data arguably benefit from provisions recently introduced in EU digital/data legislation that encourage the wider availability and more efficient sharing of data. Indeed, in order to adequately fulfil their public-interest mission to contribute to scientific advancement, it is vital that academic researchers are able to observe the digital infrastructures that permeate our contemporary society. Observability, however, hinges on the accessibility of data residing in and generated by these infrastructures. In this regard, the Institute for Information Law has produced a detailed report (**Part II**)³⁴⁹ that maps and evaluates transparency and data access provisions enshrined in EU digital/data law on their (potential) relevance for researchers. Some of these relevant legal frameworks are briefly discussed below.

Digital Services Act

A recently adopted legislative instrument that explicitly provides researchers with a relatively strong right to directly access third-party data, is the **Digital Services Act**. Article 40 of the Regulation enables “vetted researchers” to access data held by very large online platforms (VLOPs) and very large search engines (VLOSEs) for research “that contributes to the detection, identification and understanding of systemic risks in the European Union”, for instance on the platforms’ effects on fundamental rights, civic discourse and public health.³⁵⁰ Depending on how this provision will be implemented in practice,³⁵¹ it may become a valuable resource for research on the platform society, which, according to the EU legislator, is particularly important for “bridging information asymmetries and establishing a resilient system of risk mitigation”.³⁵²

³⁴³ Article 2(a) jo. Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC (i.e., the predecessor of Directive 2015/1535 mentioned in *supra* note 334).

³⁴⁴ See Recital 18 of Directive 2000/31/EC (e-Commerce Directive). For an analysis of what is considered as ‘economic activity’, reference is made to existing case law and literature, see e.g., CJEU 16 September 2016, C-484/14 (*Mc Fadden v. Sony Music*); CJEU 12 July 2012, C-138/11 (*Compass-Datenbank v. Austria*); Lundqvist 2013.

³⁴⁵ European Commission and Lundqvist 2022, p. 8.

³⁴⁶ European Commission and Lundqvist, 2022, p. 8 and references.

³⁴⁷ European Commission and Lundqvist 2022, p. 8.

³⁴⁸ *Ibid.*, p. 17-18; see also Joint statement by Research Organisations, Libraries, Repositories and University Networks 2022.

³⁴⁹ Institute for Information Law 2023b.

³⁵⁰ Article 40(4) DSA; recitals 80-83.

³⁵¹ A Delegated Act is expected to provide more guidance on the data access process, including the vetting process: <https://algorithmic-transparency.ec.europa.eu/news/call-evidence-delegated-regulation-data-access-provided-digital-services-act-2023-04-25_en>.

³⁵² Recital 96 DSA.

Open Data Directive

The **Open Data Directive** aims to maximise the re-use of data generated or collected at the expense of public budgets ('public data') for commercial and non-commercial purposes to the benefit of the European economy and society.³⁵³ Compared to its predecessor, the Public Sector Information (PSI) Directive,³⁵⁴ the Open Data Directive has a wider scope in that it not only covers traditional public sector information (i.e., data generated and collected by public sector bodies) but also documents held by certain public undertakings as well as data resulting from publicly funded research. The Directive promotes the concept of "open data" more forcefully, encouraging holders of public data³⁵⁵ to adhere to the principle of 'open by design and by default', to use open licences, and to make their data available in open formats and in compliance with formal open standards.³⁵⁶ Key principles enshrined in the Directive are that re-use must be allowed on a non-discriminatory basis and if fees are charged at all, that these must be transparent and based on (at most) the cost of dissemination. High-value datasets,³⁵⁷ such as geospatial and environmental data, are singled out in that they must be published via APIs, free of charge, in machine-readable formats and where relevant as a bulk download.³⁵⁸ Overall, the Open Data Directive opens up a large amount of public data for re-use, including by researchers.

Data Governance Act

Complementing the Open Data Directive, **Chapter II of the Data Governance Act** seeks to facilitate the access to and re-use of certain categories of 'closed' public data that fall outside the scope of the Open Data Directive and are typically not made publicly available for reasons of commercial confidentiality, statistical confidentiality, the protection of third-party intellectual property rights and the protection of personal data. While the Data Governance Act does not *oblige* public sector bodies to make such sensitive public data available for re-use,³⁵⁹ it strongly *encourages* them to take the necessary measures to make the data suitable for public access and re-use, for example by anonymizing the data and by securing licenses from intellectual property holders.³⁶⁰ Thus, in case a public sector body decides to grant access for the re-use of certain protected data, the Directive lays out the conditions under which the data sharing must take place and the principles public sector bodies must adhere to. These conditions largely mimic those of the Open Data Directive but under the Data Governance Act, public sector bodies generally have more leeway to impose restrictions, e.g., with regard to whom is granted access for re-use, for which purposes and at what terms.³⁶¹

Importantly, Chapter II of the Data Governance Act explicitly considers the interests of scientific research. It states that clear conditions for access to and use of such data are needed across the Union in order to "facilitate the use of data for European research".³⁶² Those conditions, in turn, "should be designed

³⁵³ Recitals 3-4, Article 1(1) and Article 3(1) ODD.

³⁵⁴ Directive 2003/98/EC, amended by Directive 2013/37/EU.

³⁵⁵ That is, public sector bodies and certain public undertakings, libraries (including university libraries), museums, archives, and educational establishments for higher education, and research performing organisations and research funding organisations in regard to research data, see Article 1(1)-(2) ODD.

³⁵⁶ Recitals 16-18 (open data) and recital 44 (open licences); Article 5(1)-(2) and Article 10(1); see also European Commission and Van Eechoud 2022, p. 14.

³⁵⁷ I.e., documents the re-use of which is associated with important benefits for society, the environment and the economy, in particular because of their sustainability for the creation of value-added services, applications and new, high-quality and decent jobs, and of the number of potential beneficiaries of the value-added services and applications based on those datasets, see Article 2(10) ODD.

³⁵⁸ Article 14(1) ODD.

³⁵⁹ See recital 11 DGA.

³⁶⁰ See recitals 15 and 17-18 DGA; Article 5(3)(a)(i) and Article 5(7) DGA.

³⁶¹ Compare Van Eechoud 2022, p. 29.

³⁶² Recital 6 DGA.

in a manner promoting scientific research”,³⁶³ for example by establishing that “privileging research should, as a rule, be considered to be non-discriminatory.”³⁶⁴ It further encourages public sector bodies to develop “a harmonised approach and harmonised processes to make [their] data easily accessible for the purposes of scientific research in the public interest”³⁶⁵ in accordance with the principle of ‘as open as possible, as closed as necessary’.³⁶⁶ When charging fees for re-use, public sector bodies must take measures to provide “incentives”³⁶⁷ for the re-use of sensitive public data for non-commercial purposes “such as scientific research purposes”,³⁶⁸ “in order to stimulate research and innovation”.³⁶⁹ In the specific context of fee-charging, ‘scientific research purposes’ are considered to include “any type of research-related purpose[s] regardless of the organisational or financial structure of the research institution in question, with the exception of research that is being conducted by an undertaking with the aim of developing, enhancing or optimizing products or services”.³⁷⁰ Fees charged for the re-use of public data for scientific research purposes should be “limited to the necessary costs incurred”³⁷¹ by the public sector body. All in all, the Data Governance Act aims to stimulate an environment in which protected public data can be shared and used for scientific research.

Proposed Data Act

In contrast to the Open Data Directive and the Data Governance Act, the **proposed Data Act** focuses on the sharing of data held by the *private* sector. It must be stressed that the shape and scope of the proposal are still very much in flux so that the precise impact of the Data Act on universities’ and academics’ research activities is difficult to assess at this moment. That said, there are two chapters and one provision in the Regulation that may positively affect the availability of data for scientific research purposes.

Firstly, Chapter II aims to ensure better access to Internet of Things³⁷² (IoT)-data, that is, data generated by “smart” physical devices that obtain, generate or collect data concerning their performance, use or environment and that communicate these data through the internet.³⁷³ In their capacity as users of (their own) IoT products – for instance, laboratory equipment and medical devices – academic researchers will directly benefit from the proposed product user access rights.³⁷⁴ In addition, the Chapter seems to enable researchers to indirectly access data generated by third-party IoT devices, provided that the users of those IoT products agree to request the respective data holders – often the manufactures or designers of the products – to share the IoT data with the researchers.³⁷⁵

³⁶³ Recital 15 DGA.

³⁶⁴ Ibid.

³⁶⁵ Recital 16 DGA.

³⁶⁶ Ibid.

³⁶⁷ Article 6(4) DGA jo. recital 25 DGA.

³⁶⁸ Ibid.

³⁶⁹ Incentives could take the form of discounted fees or even absent fees, see Article 6(4) jo. recital 25 DGA.

³⁷⁰ Recital 25 DGA.

³⁷¹ Recital 25 DGA. N.B. Researchers and research institutions performing research for *commercial* purposes (R&D) can be charged higher fees.

³⁷² The Internet of Things can be described as an infrastructure of physical objects that are interconnected through interoperable information and communication technologies, see International Telecommunication Union (ITU) Recommendation ITU-T Y.4000 (former ITU-T Y.2060), p. 1 and Gartner Glossary for Information Technology, <<https://www.gartner.com/en/information-technology/glossary/internet-of-things>>.

³⁷³ Recital 14 pDA. Examples of IoT-devices are smart speakers, televisions, refrigerators, thermometers, door bells, and so on.

³⁷⁴ Articles 3-4 pDA.

³⁷⁵ Article 5.

Secondly, Chapter III of the proposed Data Act sets out general obligations for data holders who are legally obliged to make data available to data recipients in business-to-business relations,³⁷⁶ addressing the conditions under which data must be made available as well as the compensation that can be requested for making the data available. As a general rule, any terms attached to the access to and use of data must be Fair, Reasonable and Non-Discriminatory (FRAND), and any compensation agreed upon must be reasonable.³⁷⁷ Thus, data holders who are legally obliged to share their data cannot unduly shield their data by implementing restrictive contractual terms. The new obligations for data holders are likely to open up more data for data recipients, including, potentially, for academic researchers. Although the Chapter primarily applies to “business-to-business relations”, it could still prove relevant for academic research, for example in the context of public-private partnerships.

Finally, Article 21 of the proposed Data Act – which covers the sharing of private sector data with public sector bodies in the event of an ‘exceptional need’ – may be used to enlist scientific research for analysing public policy issues. The provision allows that public sector bodies who received data from data holders in the context of an ‘exceptional need’ share these data with individual researchers and research organisations that operate on a not-for-profit basis or in the context of a public-interest mission when this is necessary to carry out scientific research activities or analytical activities that the public sector bodies *cannot* perform themselves. The research activities must be compatible with the purpose for which the data were requested at first (the exceptional need), and the original data holder must be informed about the data sharing.³⁷⁸ However, given that the outsourcing of research in the context of an exceptional need is not likely to happen very often in practice, it cannot be said that this provision really ‘boosts’ the availability of data for scientific research.

General Data Protection Regulation

Where datasets contain personal data, the sharing and use thereof must be in keeping with the (strict) requirements under the **General Data Protection Regulation**. However, the Regulation contains a special regime for the processing (accessing, sharing, etc.) of personal data for scientific research purposes.³⁷⁹ The notion of “scientific research purposes” is interpreted broadly and includes for example “technological development and demonstration, fundamental research, applied research and privately funded research”.³⁸⁰ According to the regime, the secondary use of personal data for scientific research must, as a rule, *not be considered incompatible* with the initial purposes of the data processing,³⁸¹ thus opening up the possibilities of the use of personal data for research purposes. Researchers and research institutions must however implement “appropriate safeguards” when using personal data, such as pseudonymisation measures, to ensure the principle of data minimisation.³⁸²

Copyright in the Digital Single Market Directive

Lastly, it could be argued that the **Copyright in the Digital Single Market Directive** also ‘opened up’ data and information for scientific research. By introducing mandatory copyright exceptions allowing for

³⁷⁶ Data holders can be legally obliged to share data on the basis of Union law or on the basis of member state legislation. Note that voluntary data sharing practices are not subjected to these rules, see recital 38 pDA. Moreover, a “data recipient” is understood as “a legal or natural person, acting for purposes which are related to that person’s trade, business, craft or profession”, see Article 2(7) pDA.

³⁷⁷ Article 8 and 9 pDA.

³⁷⁸ See Article 21(1)-(2) and (4) pDA.

³⁷⁹ Article 89 GDPR; see also, e.g., Article 5(1)(b), Article 9(2)(f) GDPR.

³⁸⁰ Recital 159 GDPR.

³⁸¹ Article 5(1)(b) GDPR.

³⁸² Article 89(1) GDPR.

the use of, notably, *lawfully accessed*³⁸³ copyright-protected works by means of Text and Data Mining (TDM) technologies, in particular for scientific research purposes, it has provided more clarity to researchers about the copyright implications of engaging in TDM.³⁸⁴ “Scientific research” in this regard is understood to cover both “the natural sciences and the human sciences”.³⁸⁵ The harmonisation has enabled TDM-research on corpora from different countries, facilitating the cross-border cooperation between researchers in the EU.³⁸⁶

Despite the newly introduced exceptions, two expert studies commissioned by the European Commission concluded that the EU copyright law framework could still be improved in order to guarantee researchers’ effective access to and re-use of data and other scientific publications.³⁸⁷ It has been claimed that researchers who seek access to copyright-protected works and databases to identify relevant data sources and compile datasets for their research, often have to comply with many legal conditions and requirements before they can finally benefit from the (narrow) legal exceptions for the scientific use of the works.³⁸⁸

It has also been argued in the literature that the scope of the scientific research exception as laid down in the **Information Society Directive**³⁸⁹ – which allows for the use of copyright-protected works “for the sole purpose of illustration for teaching or scientific research” – should be clarified: is it limited to the use of copyrighted works for “illustration” for scientific research or does it also apply to the use for the purpose of scientific research in a broader sense?³⁹⁰ In this regard it has also been argued that the scientific research exception must become mandatory (rather than optional) for all EU Member States so as to better support the research community.³⁹¹

Socio-technical processes to operationalise data sharing

Evidently, the wider availability of data *alone* does not ensure that academic researchers have easy access to such data and can effectively use it for their research. It is therefore important to also highlight recent developments under the EU’s digital policy agenda that contribute to an ‘enabling environment’ for data-driven research, in particular those enhancing the social-technical processes needed to actually share data.³⁹²

Data Governance Act

The **Data Governance Act** introduced legal frameworks on two novel data-sharing mechanisms: “data intermediation services” and “data altruism services”. **Chapter III** of the Regulation sets out a notification and supervision framework for data intermediation services, which are defined as services that “aim to establish commercial relationships³⁹³ for the purpose of data sharing between an undetermined number of data subjects and data holders, on the one hand, and data users on the other hand, through technical, legal and other means, including the exercise of data subjects’ rights in relation to personal data”.³⁹⁴ Examples

³⁸³ Notably, the exceptions concern the *use* of copyrighted works by means of TDM, not the researchers’ *access* to the works. Researchers must lawfully access copyrighted works before they can invoke the TDM provisions of the CDSM-Directive.

³⁸⁴ Article 3-4 CDSM-Directive.

³⁸⁵ Recital 12 CDSM-Directive.

³⁸⁶ Of note, there is a fair amount of criticism on the implementation of the CDSM-Directive in member states (there is still no complete uniformity) and on the limitation of the TDM-exception to reproduction (not including the “making available”-right).

³⁸⁷ European Commission and Angelopoulos 2022; European Commission and Senftleben 2022.

³⁸⁸ European Commission and Senftleben 2022, p. 64-65.

³⁸⁹ Article 5(3)(a) of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2002 on the harmonization of certain aspects of copyright and related rights in the information society (Information Society Directive).

³⁹⁰ European Commission and Angelopoulos 2022, p. 12-17, 55.

³⁹¹ *Ibid.*

³⁹² For a more in-depth discussion on how EU digital/data legislation may contribute to an enabling environment for researchers’ data access, reference is made to Institute for Information Law 2023b.

³⁹³ Of note, while providers of data intermediation services mediate commercial relationships – i.e., business-to-business and business-to-consumer relationships – they themselves could operate on a not-for-profit basis, see recital 32 DGA.

³⁹⁴ Article 2(11) DGA.

of data intermediation services mentioned in the recitals are data marketplaces (through which businesses can make data available to others), orchestrators of data sharing ecosystems that are open to all interested parties (e.g., common European data spaces), and data pools the use of which can be licensed.³⁹⁵ Data intermediation services are envisioned to promote the exchange of substantial amounts of data, which could also be relevant for scientific research.³⁹⁶ It should be noted, however, that although universities and academics could in theory be the buyers or sellers of data shared via data intermediation services, this is not likely to happen very often in practice, considering that much of the sharing that universities and academics engage in typically takes place in a not-for-profit context.³⁹⁷

AMdEX: data intermediation or data altruism?

AMdEX (Amsterdam Data Exchange) is a joint initiative of the University of Amsterdam, SURF,³⁹⁸ AMS-IX,³⁹⁹ Dexes⁴⁰⁰ and the Amsterdam Economic Board,⁴⁰¹ co-funded by the European Union and the Dutch Province of Noord-Holland which aims to set up a neutral exchange infrastructure – a “digital notary”⁴⁰² – to facilitate data sharing.⁴⁰³ AMdEX has been testing various digital marketplaces, for instance for aircraft maintenance data to be shared between airlines;⁴⁰⁴ sensor data collected in smart buildings to be shared with facility service providers and mobility planners; and data resulting from research to be shared between researchers and with industry.⁴⁰⁵ A prototype of the latter marketplace, the “Research Data Exchange” (RDX), was made available in 2021 and is currently being developed further.⁴⁰⁶ As AMdEX plans to facilitate both commercial and non-commercial data exchanges, the question is to what extent this hybrid mechanism is subject to the rules for data intermediation services.⁴⁰⁷

Chapter IV of the Data Governance Act appears to be more relevant to the university context. The Chapter lays down a registration scheme for organisations facilitating “data altruism”. Contrary to data intermediation services, data altruism services do *not* aim to establish commercial relationships between data holders and data users. Data altruism, as a practice, refers to the “voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensations related to the costs that they incur when making their data available for objectives of general interest as provided for in national law (...)”.⁴⁰⁸ Legal entities that want to be registered as recognised data altruism organisations *must* operate on a not-for-profit basis, but commercial entities can in principle be users of such data.⁴⁰⁹ As re-users of data, universities and academics are likely to benefit from the new rules on data altruism, the practice of which is expected to contribute to the emergence of pools of valuable data which can also be used for scientific research.⁴¹⁰ Universities could even set up data altruism organisations themselves if public funding allows for it.

³⁹⁵ Recital 28 DGA.

³⁹⁶ Recital 27 DGA.

³⁹⁷ European Commission and Van Eechoud 2022, p. 28, 30.

³⁹⁸ The collaborative organisation for IT in Dutch education and research, see <<https://www.surf.nl/en>>.

³⁹⁹ Amsterdam Internet Exchange, a member-based association that operates multiple interconnection platforms worldwide, see <<https://www.ams-ix.net/ams/about-ams-ix>>.

⁴⁰⁰ A Dutch start-up that facilitates the sharing of data between public and private entities, see <<https://www.dexes.nl/>>.

⁴⁰¹ A network of organisations, companies, educational and research institutions, municipalities, provinces and societal organisations working together on a smart, green and healthy future of the Amsterdam metropole area, see <<https://amsterdameconomicboard.com/wie-zijn-we/>>.

⁴⁰² AMdEX news, <<https://amdex.eu/news/data-exchange-game-and-powerful-insights/>>.

⁴⁰³ About AMDeX (webpage), <<https://amdex.eu/about/>>.

⁴⁰⁴ Van Wijnen and Olsthoorn 2021.

⁴⁰⁵ See <<https://amdex.eu/usecases/>>.

⁴⁰⁶ By the University of Amsterdam and SURF. See <<https://rdx.lab.surf.nl/access/10.21942/uva.17104532>>.

⁴⁰⁷ European Commission and Van Eechoud 2022, p. 31.

⁴⁰⁸ Article 2(16) DGA.

⁴⁰⁹ Article 18(c) DGA. National implementations of the registration scheme are currently underway, but some unclarity remains about the exact conditions on which registration can be obtained.

⁴¹⁰ European Commission and Van Eechoud 2022, p. 31.

Data donation to academic research

Over the years, “data donation” has become a popular mechanism among researchers as a means to access individuals’ digital traces and use them for research.⁴¹¹ At the University of Amsterdam, researchers have been developing a web-based data donation platform where participants in research projects can upload (parts of) (anonymised) personal data exports from online platforms – generally obtained using the data access right under the General Data Protection Regulation – to a specific research project.⁴¹² Provided that the data donations on such platforms are voluntary, are based on the consent of data subjects (in case of personal data) or the permission of data holders (in case of non-personal data), and are provided free of charge or against marginal costs, universities and other not-for-profit research institutes operating such platforms could qualify for registration as “data altruism organisations recognised in the Union”.⁴¹³

European Open Science Cloud (EOSC)

Another important development is the emerging European Open Science Cloud (**EOSC**) which is designated as a socio-technical facility to share research data and other research-related resources. Not only will it provide technical infrastructure, but it also aims to develop additional arrangements such as licensing models and interoperability guidelines⁴¹⁴ to streamline data sharing. Currently, the EOSC is mainly framed – as the name suggests – as an environment to support open science,⁴¹⁵ that is, a vehicle to share and access research data and other digital research objects (data *output*, see section 4.2.4), and not so much as a mechanism for researchers to access data that are held by third parties (governments, private sector companies) which can be used as *input* for scientific research. Nevertheless, it is a promising vehicle which could potentially also contribute to the governance of access to third-party data for research purposes, for instance by providing secure processing environments as foreseen under the Data Governance Act.

Proposed Data Act

A last development worth highlighting in this regard is the legislative proposal for a **Data Act**. Its second chapter on Internet-of-Things (IoT) data contains a provision which would allow users of IoT-products to request the data holder (often the manufacturer of the product) to make the data generated by the use of their IoT devices available to designated third party.⁴¹⁶ This special type of ‘data portability’ holds potential for the seamless sharing of IoT-data for scientific research purposes. While the notion of data portability was originally conceived to overcome technology-and-vendor lock-ins and to grant data subjects control over their personal data (see section 4.2.1), this particular arrangement for data porting in the proposed Data Act can be seen as a new socio-technical mechanism to support the sharing of data outside of the data relationship between data holder and user of IoT-products.

4.2.4 Provision of research data (data output)

While EU law has afforded universities and academics – among many other actors – legal entitlements enhancing their access to data in their role as data users, at the same time it has also imposed a number of

⁴¹¹ E.g., the “Data for Good”-initiative, <https://dataforgoodfoundation.com/en/> (Denmark) and the Corona Data Donation App, <https://corona-datenspende.de/science/en/> (Germany).

⁴¹² Araujo et al 2022; see the source code at <https://github.com/uvacw/osd2f>. Araujo is now developing a national ‘digital data donation infrastructure (D3I)’, see: <https://www.uva.nl/en/shared-content/faculteiten/en/faculteit-der-maatschappij-en-gedragwetenschappen/news/2021/12/six-dutch-universities-start-data-donation-project.html>.

⁴¹³ See the requirements for registration in Article 18 DGA.

⁴¹⁴ See e.g., the ‘EOSC Interoperability Framework’ (EOSC-IF), <<https://eosc-portal.eu/eosc-interoperability-framework/about-eosc-interoperability-framework-governance-eosc-if>>.

⁴¹⁵ See <<https://eosc-portal.eu/>>.

⁴¹⁶ Article 5 pDA.

new legal obligations on them in their capacity as data *holders*.⁴¹⁷ Indeed, in the course of their research, academic researchers typically collect and/or produce “research data”, which may include statistics, results of experiments, measurements, observations resulting from fieldwork, survey results, interview recordings, images and more.⁴¹⁸

In 2019, the **Open Data Directive** introduced a new provision on the accessibility and re-use of research data. The provision requires Member States to develop national open access policies to be addressed to research performing organisations – including universities’ research branches⁴¹⁹ – and research funding organisations, aimed at making research data resulting from publicly funded research “openly available” (accessible).⁴²⁰ The provision further prescribes that publicly funded research data that have been made publicly available through institutional or subject-based repositories, must subsequently be made “re-usable” for commercial and non-commercial purposes.⁴²¹ The general conditions for re-use of all manner of public sector information laid down in Chapters III-IV of the Directive similarly apply to research data.⁴²² While the research data provision itself does not specify which research stakeholders are the bearers of the obligation to enable re-use, it seems likely that – looking at scientific practice and anticipating the open access policies mentioned above – Member States, in their national laws, will place the responsibility for allowing re-use on research performing organisations, including universities.⁴²³ According to the Directive, the re-use of publicly funded research data should in principle not be subjected to conditions unless these conditions are necessary and proportionate to public interest objectives.⁴²⁴ In this respect, the use of open and standardised licenses is strongly encouraged.⁴²⁵ It is already the case that major science funders and publishers increasingly require researchers to use (standard) open licenses for the sharing of their research data, most notably the (very) liberal Creative Commons ‘CC0’ and ‘CC BY’ licenses.⁴²⁶ These licenses allow anyone, anywhere, the unrestricted use of the data for any purpose, forever. The use of open licenses is likely to grow further now that it is backed by EU law.

Complementing the Open Data Directive, **Chapter II of the Data Governance Act** lays down a framework for the re-use of data held by public sector bodies that are ‘protected’ on grounds of commercial confidentiality, statistical confidentiality, third-party intellectual property rights and the protection of

⁴¹⁷ For a more in-depth contribution on the ‘institutionalisation’ of research data sharing at the EU-level, reference is made to Van Eechoud 2023.

⁴¹⁸ Recital 27 ODD.

⁴¹⁹ European Commission and Van Eechoud 2022, p. 30 and recital 28 of the Open Data Directive: “Research performing organisations and research funding organisations could also be organised as public sector bodies or public undertakings. This Directive applies to such hybrid organisations only in their capacity as research performing organisations and to their research data.”

⁴²⁰ Article 10(1) ODD. Thus, the Directive as such does *not directly impose* an obligation on research performing organisations to make research data openly available (accessible), e.g., in repositories; this is however *implied* by the obligation imposed on Member States to adopt open access policies which must be *addressed* to research performing organisations.

⁴²¹ Article 10(2) ODD.

⁴²² Article 10(2) ODD. Please note that Chapter II of the Directive does not apply to research data; research performing organisations do not have to process requests for re-use (but they may do so voluntarily).

⁴²³ European Commission and Van Eechoud 2022, p. 24. See for example, Article 5b of the Dutch legislative proposal implementing the Open Data Directive, which explicitly provides that “the publicly funded research organisation” (de *publiek gefinancierde onderzoeksorganisatie*) must actively make its research data re-usable, insofar as the data (a) have been generated in the course of fully or partially publicly funded research activities, (b) have been made publicly available via an institutional or thematic repository, and (c) legitimate commercial interests, knowledge transfer activities and pre-existing intellectual property rights do not conflict with the re-use.

⁴²⁴ Article 10(2) jo. Article 8(1) ODD.

⁴²⁵ Recital 44 ODD: “Open licences in the form of standardised public licences available online which allow data and content to be freely accessed, used, modified and shared by anyone for any purpose, and which rely on open data formats, should play an important role in this respect. Therefore, Member States should encourage the use of open licences that should eventually become common practice across the Union.”

⁴²⁶ See, for example, the European Commission in the context of Horizon Europe grants (CC BY, CC0 or equivalent licenses), <https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/aga_en.pdf>; European Council for Nuclear Research (CC0 waiver), <<https://opendata.cern.ch/docs/terms-of-use>>; Elsevier/Mendeley Data (CC0, CC BY or CC BY-NC), <https://service.elsevier.com/app/answers/detail/a_id/14316/supporthub/publishing/~/-/which-license-should-i-select-when-posting-my-research-data%3F/>.

personal data.⁴²⁷ In contrast to the Directive, the Data Governance Act does not distinguish between research data and non-research data, and does not contain a special regime for (publicly funded) research data either. However, according to recital 12 of the Regulation, public research performing organisations – including, as it would seem, the research branches of universities that are organised as public sector bodies or bodies governed by public law – seem to fall under the re-use rules with respect to certain exchanges of their (research) data.⁴²⁸ Thus, in case universities hold (research) data that are protected on the abovementioned grounds, they may decide for themselves whether they allow re-use or not (see section 4.2.3). If they do, they must comply with the conditions and principles laid down in articles 4-9 of the Data Governance Act.

While the new obligations to enable open access to and the re-use of publicly funded research data are applaudable from the perspective of open science, they are not without consequences. The obligations come with an administrative burden which ultimately lands on the plate of individual academic researchers (and support staff) who have to prepare the research data for publication and re-use. One particular challenge is that for each dataset, it must be established which, if any, legal constraints there are to make them accessible, and what this means for the way in which they are made available, for instance in terms of security measures and license types. This requires, amongst other things, that the provenance and legal properties of the data are clear. The Open Data Directive prescribes that when data are made openly available, concerns relating to intellectual property rights, personal data protection and confidentiality, and security and legitimate commercial interests must be taken into account in accordance with the principle of ‘as open as possible, as closed as necessary’.⁴²⁹ This balancing act between open research data and third-party interests can be a real challenge for individual researchers. Considerations of data protection, for instance, may lead to complicated decisions since the **General Data Protection Regulation** requires a high level of protection of Europeans’ personal data. Taking measures to ensure compliance with data protection requirements such as anonymisation or pseudonymisation can be a time- and knowledge-intensive task. Moreover, datasets can be large and complex, and may require hours of preparatory work (indexing, cleaning up, formatting) before they can be uploaded to a publicly available repository. In order to render data ‘FAIR’,⁴³⁰ datasets must be accompanied with (detailed) metadata to describe them and explain how they should be used. Preparation of metadata also requires time, effort and skills.⁴³¹

During the legislative process of the Open Data Directive, the European Commission acknowledged the potential administrative burden associated with the sharing of research data. However, back in the days the Commission argued that the impact of the new research data provision would remain limited since the re-use obligation only applies to data “for which researchers[s] [have] already made all relevant efforts in order to make the data publicly accessible (...) in particular through web-based repositories that are designed to automate the dissemination process, making any intervention by the researcher[s] unnecessary.”⁴³² Whether this is a strong argument can, however, be debated. The efforts that have to be made to make research data publicly accessible in the first place cannot be overlooked when assessing the impact of the re-use obligation, especially considering that the Open Data Directive requires Member States to adopt open access policies to compel researchers into openly sharing their data.

⁴²⁷ Article 3(1) DGA.

⁴²⁸ See recital 12 DGA: “Research-performing organisations and research-funding organisations could also be organised as public sector bodies or bodies governed by public law. This Regulation should apply to such hybrid organisations only in their capacity as research-performing organisations.” Please note that “the exchange of data between researchers for non-commercial scientific purposes” is not covered by the re-use obligations laid down in Chapter II (recital 12, last sentence). See also Van Eechoud 2022, p. 30.

⁴²⁹ Article 10(1) ODD.

⁴³⁰ FAIR data are data which meet principles of findability, accessibility, interoperability, and reusability (FAIR); see M.D. Wilkinson, M. Dumontier, Ij. J. Aalbersberg, et al. ‘The FAIR Guiding Principles for scientific data management and stewardship’, *Scientific Data* 2016, Vol. 3, No. 1.

⁴³¹ European Commission Horizon 2020 Monitoring Report 2017, p. 72.

⁴³² European Commission, Proposal for a Directive on the re-use of public sector information (recast), COM(2018) 234 final, 24 April 2018, p. 8.

Average time spent making research data available

The German Federal Statistical Office estimated in 2021 that a German federal research agency, on average, processes about 265,000 research datasets per year. Extrapolated to 43 federal research agencies, this amounts to 11.4 million datasets. Of those datasets, 10.2 million datasets are considered to be subject to the re-use obligation (taking into account third-party interests of personal data protection, copyright, security-sensitive information, etc.). Assuming that on average, scientific publications are accompanied with 50 datasets, this comes down to a total of 205,000 dataset-uploads per year. The Statistical Office assumed that a large part of the data produced and collected by researchers is usually already prepared for publication and re-use *during* the research projects, considering that research institutions have an obligation to pursue good research practice. Nevertheless, it can be argued that *after* completion of a research project and *before* the publication of the results, the underlying datasets must be checked, at least randomly. The Statistical Office estimated that this check generally takes about 37 minutes. After that, the datasets must be uploaded to a repository (made publicly available). The Statistical Office gauged that after one year of practice, a routine will be established so that the upload of datasets by researchers will eventually take 5 minutes per upload. The total average time to prepare research data and make them available thus amounts to $(37 + 5 =) 42$ minutes per upload.⁴³³ Notably, this is *not* including the time already spent during the research project to organise the research data and make them suitable for analysis *nor* the time spent to prepare the metadata. The number does also not differentiate between different fields and types of research.

Time and efforts can be translated into monetary costs, and thus, a financial burden. The deposit, storage and maintenance of large amounts of data in publicly accessible repositories requires considerable storage space and qualified staff.⁴³⁴ However, many universities do not yet have sufficient expertise, technologies and infrastructure in place to routinely facilitate successful re-use.⁴³⁵ Substantial investments in open research data support are therefore necessary, which will create pressure on universities' resources. Some experts even propose that 5% of all research costs should be spent on data stewardship, which for all EU Member States combined would amount to approximately 15 billion euros per year.⁴³⁶ A fear among academics is that the funding of open research data – which inevitably has to be provided by research funding and state budgets because at the moment “the benefits of open research data (...) are largely hypothetical or only beginning to materialise”⁴³⁷ – will eat up the funding available for research and teaching, and manifest as a new type of ‘overhead costs’.⁴³⁸

Besides practical arguments of time, effort and a lack of practical facilities, individual researchers may have more fundamental reasons why they prefer not to share certain research data. A fear of misinterpretation or misuse of data for objectives inconsistent with human rights and/or public values, or a lack of credit or recognition, are frequently mentioned in scholarly literature as inhibitors of open research data sharing.⁴³⁹ There may also be situations where the prerogative of open science and open research data may (at least temporarily) conflict with universities' and/or researchers' aspiration to obtain intellectual property rights, such as patents for their innovations, in order to commercially license them.⁴⁴⁰ And while

⁴³³ Explanatory Memorandum to the German proposal implementing the Open Data Directive (Entwurf eines Gesetzes zur Änderung des E-Government-Gesetzes und zur Einführung des Gesetzes für die Nutzung von Daten des öffentlichen Sektors), p. 22-23. Available at: <<https://dserver.bundestag.de/btd/19/274/1927442.pdf>>.

⁴³⁴ European Commission Horizon 2020 Monitoring Report 2017, p. 12-13.

⁴³⁵ Mons 2020.

⁴³⁶ Mons 2020; EU Member States spent around €311 billion and €328 billion in 2020 and 2021 respectively, see <<https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20211129-2>> and <<https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20221129-1>>.

⁴³⁷ Kitchin 2014, p. 66.

⁴³⁸ Mons 2020; Van Dijck, Poell and De Waal 2018, p. 134.

⁴³⁹ For a comprehensive overview of the drivers and inhibitors of research data sharing distilled from existing literature: Zuiderwijk, Shinde and Jeng 2020.

⁴⁴⁰ Under European patent law, the public disclosure of ideas prior to making a patent application must be avoided. Non-disclosure runs however counter to open science principles. See ALLEA Statement on IPRs and Open Science 2022, p. 6.

trade secrets’ are rarely invoked by research-performing organisation and academics, research collaborations with private sector actors may involve trade secrets in relation to research data.⁴⁴¹

One could wonder to what extent open research data sharing requirements, as brought forth by the EU’s Open Science Policy and specifically the Open Data Directive, can always be justified in light of academic freedom and institutional autonomy.⁴⁴² Not only may such requirements conflict with researchers’ self-determined course of action in deciding whether, when, where and under which conditions their data are published, they arguably also infringe upon universities’ financial autonomy by forcing them to substantially invest in research data management. The EU legislator must ensure that the balance between promoting open science and protecting the rights and freedoms of universities and individual researchers is upheld.

4.2.5 Connection with digital sovereignty

The subsections above identified some of the rights and obligations for universities and academic researchers resulting from EU legislation adopted under its Open Science Policy as well as its broader policy in the field of data, digital technologies and AI. The current surge of legislative action significantly affects the legal environment in which universities and academics operate and carry out scientific research. In certain respects, the new wave of legislation *strengthens* their digital sovereignty, while in others, their digital sovereignty is rather (unintentionally) *weakened*.

First of all, EU digital/data legislation can strengthen research organisations’ digital sovereignty without necessarily targeting the research sector – although the onus of realising digital sovereignty claims vis-à-vis digital technology suppliers is typically on them.⁴⁴³ For instance, EU legislation that requires digital services to be interoperable and to enable data portability could reduce technology- and vendor-lock-ins, backing the position of the customer of these covered services and infrastructures.⁴⁴⁴ Moreover, universities can leverage the General Data Protection Regulation to discipline suppliers’ practices that extract excessive amounts of personal data from end-users of universities’ digital infrastructures and services.⁴⁴⁵ The caveat remains, however, that oftentimes the digital services markets are too concentrated to be disciplined by competitive forces, and that universities as clients of big tech have to be very strategic when procuring digital services and infrastructures. Furthermore, universities and academics in principle benefit from the wider availability of data and enhanced socio-technical processes facilitating data-sharing.⁴⁴⁶ This primarily concerns the re-use of public sector data, with additional categories of protected data held by public sector bodies becoming available (subject to specific safeguards). By extension, EU copyright law and data protection law hold privileges for using data that have been lawfully obtained in the first place.

Secondly, although EU digital/data law does not intentionally weaken the digital sovereignty of universities and academics, it does increase their burden of compliance in certain respects. Without prejudice to the respectable objectives of the EU’s Open Science Policy, the production and management of open research data is a heavy responsibility weighing on public research organisations that demands considerable efforts and resources. To be sure, European universities fully back the overarching policy objective of open science and are generally supportive of opening-up research data for re-use. Yet, EU policymakers tend to downplay the impact that the EU’s Open Science Policy has for universities and academics in terms of labour and resources required to comply with the Open Data Directive and the Data Governance Act. Considering that open research data sharing generates a new type of ‘overhead expenses’ for universities and other research-performing organisations, it will be important to better recognise this in

⁴⁴¹ See Rajam 2020.

⁴⁴² Van Eechoud 2022, p. 19, 43.

⁴⁴³ Roosendaal 2023.

⁴⁴⁴ See *infra* sections 3.2.1 and 4.2.1.

⁴⁴⁵ See *infra* sections 3.3.1 and 3.4.

⁴⁴⁶ See *infra* section 4.2.3.

the Open Science Policy and public research funding. It will also be key to develop and scale up appropriate data sharing institutions, including the European Open Science Cloud (EOSC). While the obligation to share research data in view of open science is clearly defined, there is (some) legal uncertainty about universities' and academics' obligations arising from regulations adopted under the EU's broader digital policy agenda. For instance, it is still open to debate to what extent the Digital Services Act applies to digital technologies and infrastructures provided by universities (e.g., repositories, discussion forums) since scientific research is not clearly addressed. Similarly, it must be confirmed to what extent the new AI Act will apply to AI systems developed and used for scientific research purposes.

Building on the (not exhaustive) mapping of rights and obligations, the next section highlights the EU's piecemeal recognition of freedom of science and scientific research in its digital and data law, leading to legal incoherence and uncertainty. While this shortcoming may not affect the digital sovereignty of universities and academics *per se*, it is argued that the EU should change the way in which it currently addresses scientific research to do justice to universities' interests and academic values.

4.3 Recognition of universities' interests and academic values in EU law and policy

Looking at the legislative developments in the digital and data domain, several universities, university associations and academics have expressed grave concern regarding the way universities are currently treated at the EU-level. The general feeling is that the unique role, interests and responsibilities of universities have not been sufficiently recognised by the EU legislator, and that they are wrongfully approached like market sectors.⁴⁴⁷ For example, in the working documents accompanying legislative proposals, research-performing organisations such as universities are rarely identified as relevant stakeholders.⁴⁴⁸ This seems to indicate that EU law- and policymakers do not see universities as full participants in the discussion on the digital transformation, even though they are confronted with new legal obligations just like other societal actors. Furthermore, while the notion of “scientific research” features here and there in EU legislation (see below), the broader value of academic freedom still appears to be quite under the radar in EU law and policy. The recently signed European Declaration on Digital Rights and Principles for the Digital Decade⁴⁴⁹ is a striking example of this: while it is said to cover “key rights and principles for the digital transformation” in the Union,⁴⁵⁰ academic freedom is not included as such. University associations and academics have argued that the EU's holistic approach⁴⁵¹ to challenges related to digitalisation and data disregards the distinct situation and needs of universities that set them apart from commercial for-profit companies. According to them, this lack of differentiation hinders the creation of a knowledge society fit for the digital age.⁴⁵² This is not to say, of course, that blanket legislation can never be justified – universities acknowledge that in some cases, it may be needed⁴⁵³ – but it is strongly emphasised

⁴⁴⁷ E.g., Joint statement of CESAER, COAR and LIBER 2022, p. 1; LERU Data Statement 2021, p. 1; Luyben, in: LERU New Year's Debate 2022 (01:39:30 and further); see also Devolder, in LERU New Year's Debate 2022 (00:58:35 and further); Maex 2021, p. 4.

⁴⁴⁸ Devolder, in LERU New Year's Debate 2022 (00:58:35 and further). See also Ehler, in: Academic Freedom Roundtable 2023 (16:19:20-16:19:55), noting that “there [has been] no impact assessment from the Commission to what extent a regulation impacts scientific freedom”. Notably, the Open Data Directive does provide a definition of ‘university’ – “any public sector body that provides post-secondary school higher education leading to academic degrees”, Article 2(4) ODD – but does however does not distinguish between the distinct functions they perform, i.e., education, research and libraries.

⁴⁴⁹ Available at: <<https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles>>.

⁴⁵⁰ European Commission, ‘Commission puts forward declaration on digital rights and principles for everyone in the EU’, 26 January 2022, <https://ec.europa.eu/commission/presscorner/detail/en/IP_22_452>.

⁴⁵¹ Devolder, in LERU New Year's Debate 2022 (00:58:35 and further).

⁴⁵² Joint statement of CESAER, COAR and LIBER 2022, p. 2; Luyben, in: LERU New Year's Debate 2022 (01:48:40 and further); see also Devolder, in LERU New Year's Debate 2022 (00:58:35 and further).

⁴⁵³ Luyben, in: LERU New Year's Debate 2022 (01:48:40 and further).

the EU legislator should be more cognisant of the consequences of economic regulation for academic freedom of universities and academics in the Union.

4.3.1 *The notion of “scientific research” in EU legislation*

The term “scientific research” (or alternatively, “scientific research purposes”) occasionally features in EU digital and data legislation. It is mainly used in the context of exceptions to rules, or, in the case of the Open Data Directive and Data Governance Act, obligations that aim to promote the circulation of scientific knowledge and research data in society. To date, however, there is no harmonised EU definition of scientific research; its meaning and possibly scope varies by legislative instrument.

When EU legislation *privileges* research activities, it gravitates around two models. Under the first model, ‘research’ comprises both **not-for-profit scientific** research and **commercial** research and development. The General Data Protection Regulation, for example, adopted such a broad interpretation that is not limited to “fundamental research” but also encompasses “technological development and demonstration”, “applied research” and “privately funded research”.⁴⁵⁴ Additionally, the proposed AI Act will most likely not apply to scientific research nor to commercial research, which would leave research activities unregulated up to the point that an AI system is put into circulation. Under the second model, legal privileges for research are designed to benefit exclusively public interest-driven and/or not-for-profit scientific research. The Copyright in the Digital Single Market Directive, for instance, refers to scientific research covering “both the natural sciences and human sciences”⁴⁵⁵ and distinguishes between research organisations acting on a not-for-profit basis or in the context of a public-interest mission, and organisations operating under commercial influences. The latter organisations may not rely on the copyright exception for text and data mining research.⁴⁵⁶ Lastly, while the Information Society Directive does not define the notion of scientific research as such, it does specify that its copyright exception for research only applies to “non-commercial purposes”.⁴⁵⁷

In the context of the EU’s Open Science Policy, *legal obligations* and best practices concerning open research data sharing primarily concern **publicly funded** research. The Open Data Directive, for instance, opens-up research data resulting from scientific research activities “subsidised by public funding or co-funded by public and private-sector entities.”⁴⁵⁸ A similar approach can be found in the Data Governance Act, which defines scientific research purposes as “any type of research-related purpose regardless of the organisational or financial structure of the research institution in question, with the exception of research that is being conducted by an undertaking with the aim of developing, enhancing or optimising products or services.”⁴⁵⁹ Corporate research and development activities thus fall outside the scope of this definition.

From the point of view of public interest-oriented research organisations, it would be preferable if the EU (co-)legislator consolidates its notion of “scientific research” and applies it consistently across EU legal instruments. The approach taken in the Copyright in the Digital Single Market Directive, which is well-crafted and fit for purpose, could be considered as a template for defining “scientific research”. Legal exceptions and privileges should be exercised in accordance with recognised ethical standards for scientific research as is required in the General Data Protection Regulation and the proposed AI Act. Additional

⁴⁵⁴ Recital 159 GDPR. Note that some member state legislation implementing the GDPR, including the Dutch *Uitvoeringswet algemene verordening gegevensbescherming* (UAVG), have declared the research exception of Article 9(2)(j) GDPR applicable only to scientific research that serves the *public interest*, and not to commercial research. See Article 24 UAVG. Moreover, the European Data Protection Supervisor (EDPS) has indicated he considers the special data protection regime for scientific research to be applicable only when “the research is carried out with the aim of growing society’s collective knowledge and wellbeing, as opposed to serving primarily one or several private interests”, see EDPS Preliminary Opinion 6 January 2020, p. 12.

⁴⁵⁵ Recital 12 CDSM-Directive.

⁴⁵⁶ Recital 12 CDSM-Directive.

⁴⁵⁷ Article 5(3)(a) jo. recital 42 InfoSoc-Directive.

⁴⁵⁸ Recital 28 ODD.

⁴⁵⁹ Recital 25 DGA.

guidance on what ethical standards for scientific research should entail in the digital era will be important in order to operationalise these notions. This is not to say, however, that for-profit and commercial research and development can never be considered a privileged research activity inside EU law, but these activities should not be conflated with public-interest driven scientific research.

4.3.2 Targeted EU legislative intervention?

Due to the perceived undervalued role of the university sector, scientific research and knowledge infrastructures in EU digital policy and legislation, some members of the European academic community have expressed their support for “an agenda designed to protect the position of universities” and even for the development of a special “Digital University Act” – which elsewhere has also been referred to as a “European Digital Knowledge Act” – to secure universities’ independence in the rapidly digitalising and commercialising academic landscape.⁴⁶⁰ Former Rector Magnificus of the University of Amsterdam, Prof. Karen Maex, was the first to put forward the idea for such an Act, which, unlike other instruments adopted under the EU digital policy agenda, would address the particular needs of EU-based universities in the digital age. According to Maex, a Digital University Act would aim to facilitate public storage of and access to research data organised by universities and public infrastructure; freely accessible university research publications without high publication fees or private company lock-ins; control over (the development of) digital learning and research tools and the gathering and processing of user data by such tools; and access to platform data for teaching and research.⁴⁶¹

It goes without saying that universities are key institutions for the future of Europe and require public support for their digital transformation and development of strategic capacity. The proposal of a Digital University Act is laudable in that it would specifically address the problems that universities see themselves confronted with. It could also be argued that regulation which gives due prominence to the unique context of public-interest research and education is much needed to boost fundamental changes that perhaps cannot be easily achieved by voluntary and bottom-up approaches only.⁴⁶² On the other hand, it could be argued that additional legislation is not necessarily desirable in an already complex legal landscape,⁴⁶³ and that a range of problems could also be addressed without a dedicated legislative framework in place, for example at the level of universities themselves. Ultimately, what matters is that we, as a society, jointly set limits and conditions to curb the power of commercial digital technology providers over public organisations⁴⁶⁴ in order to foreclose the hollowing out of the public university-mission.

At the level of the European Parliament, academic freedom recently gained considerable traction⁴⁶⁵ and the first discussions on the need and form of “a European regulation on the freedom of scientific research”⁴⁶⁶ have been held. While envisioned as a broader instrument to protect academic freedom (in

⁴⁶⁰ Maex 2021, p. 4-5, endorsed by e.g., Luyben (EOSC), in: LERU New Year’s Debate 2022 (01:42:40 and further), and the Conference of European Schools for Advanced Engineering Education and Research (CESAER), the Confederation of Open Access Repositories (COAR) and the Association of European Research Libraries (LIBER). In their joint statement titled ‘Scientific knowledge must be protected to ensure a Europe fit for the digital age’ of 24 January 2022, the three organisations have stressed the need for a legally binding framework in the form of a ‘*European Digital Knowledge Act*’. Compare also Deketelaere 2021, who has argued for the creation of a ‘*European Knowledge Act*’ in order to finally realise “a European Knowledge Area” where knowledge can truly circulate freely, and to allow the knowledge sector “to escape unintended consequences of other pieces of EU legislation”.

⁴⁶¹ Ibid.

⁴⁶² Compare Deketelaere 2021, who has argued that “two decades of ERA policy and two years of EEA policy have shown that a voluntary, bottom-up approach is futile” to establish a true European Knowledge Area.

⁴⁶³ E.g., the LERU Data Statement 2021, p.1, on the need “to avoid the problem of over-regulation”.

⁴⁶⁴ Maex et al 2019.

⁴⁶⁵ E.g., the study into the state of play of academic freedom in EU Member States by Maassen et al (STOA, European Parliament) 2023.

⁴⁶⁶ During the first Academic Freedom Roundtable organised by the European Parliament’s Panel for the Future of Science and Technology (STOA) on 27 April 2023, the European Parliament’s Committee on Industry, Research and Energy (ITRE) announced its plan to draft a legislative own-initiative report on the freedom of scientific research and propose a text for a

particular scientific research⁴⁶⁷) and not specifically aimed at tackling threats resulting from the digitalisation and commercialisation of the university sector,⁴⁶⁸ universities and academics may be able to derive protection from such a regulatory framework. What is certain is that the piecemeal recognition of scientific research in EU regulation makes legal compliance for universities unnecessarily complex and does not provide legal certainty and joint-up guarantees to research performing organisations in the Union.

4.3.3 *Anchoring scientific research into EU law*

What emerges from the review of EU legislation on digital technologies and data, is that EU law and policy should treat scientific research as a horizontal policy objective – as laid down in EU primary law – which is also relevant in connection with, and can be affected by, EU economic regulation. While it may not be necessary to adopt a law specifically dedicated to the freedom of sciences and research, the following policy measures would already address many of the shortcomings to the way EU law and policy currently considers scientific research identified in this study.

Firstly, the EU (co-)legislator should adopt a consistent notion and definition of scientific research that emphasises the not-for-profit and public interest-oriented nature of scientific research and correspondingly links it to adherence to recognised ethical standards for scientific research as well as open science policy (including open research data). In other words, societal actors can only claim to carry out ‘scientific research’ if they also adhere to accepted research ethical standards and engage in the sharing of scientific publications and research data. The notion of scientific research and the definition of covered research organisations should be distinguished from commercial and for-profit research and development. Mixed situations such as public-private research partnerships must also be considered as to whether their activities meet the ethical requirements of scientific research.

Secondly, EU law and policymakers should give better recognition to the freedom of sciences and scientific research throughout the broader EU policy cycle. This recognition should not be strictly limited to the policymaking in the field of science but should also extend to economic regulation that can affect universities and academics. The best avenue to firmly anchor freedom of sciences and scientific research into EU policymaking would be to incorporate these values in the European Commission’s Better Regulation Guidelines and Toolbox.⁴⁶⁹ This way, research performing organisations become recognised as stakeholders also in connection with economic regulation that could affect scientific research, and the

European regulation on the freedom of scientific research (webstream: 15:12:55-15:13:13). The ITRE Committee suggests a “light-touch legal framework” aimed at making existing legal standards as enshrined in jurisprudence and other frameworks “more visible and easier to enforce” (see also Ehler 2023). The reactions from the academic community – represented in the roundtable by the European Federation of Academies of Sciences (ALLEA), the Deutsche Forschungsgemeinschaft (DFG), the European University Association (EUA), the League of European Research Universities (LERU) and the European Council of Doctoral Candidates and Junior Researchers (Eurodoc) – were mixed. All representatives pointed at the complexity of the notion of academic freedom, including scientific freedom, and the fact that threats to academic freedom come in many different forms, thus making it difficult to address the topic with a single legislative instrument. At the same time, it was agreed that EU action in this field should not be “dead by complexity” and that a “regulatory backbone” could well be complemented by other, non-legislative measures such as an annual monitoring exercise. Webstream available at:

<<https://www.europarl.europa.eu/thinktank/en/events/details/freedom-of-scientific-research-and-its-1/20230330WKS05181>>.

⁴⁶⁷ It was noted that the European Commission has to date viewed the (legal) protection of academic freedom mainly as “a higher education issue”, an area in which the European Union “has no legislative competences” (webstream: 15:11:30-15:11:52). Indeed, in accordance with the subsidiarity principle, higher education policies are decided at the level of individual Member States, while the EU only has a supporting and coordinating role (ex. Article 165(1) of the Treaty on the Functioning of the European Union (TFEU)). However, it was emphasised by ITRE that “academic freedom is not only higher education policy” but “also science policy”, and therefore “something the Union could legislate on” (webstream: 15:11:52-15:12:39).

⁴⁶⁸ However, one representative did comment during the roundtable that “academic freedom in the digital age cannot be considered along the same paradigms as in the analogue age” for the reason that “knowledge in the digital age is a common good” while “in the age of the book it was something stewarded by the individual author”.

⁴⁶⁹ European Commission, ‘Commission Staff Working Document: Better Regulation Guidelines’, SWD(2021) 305 final and European Commission, ‘Better Regulation Toolbox’, July 2023. Both available at: <https://commission.europa.eu/law/law-making-process/planning-and-proposing-law/better-regulation/better-regulation-guidelines-and-toolbox_en>.

European Commission's methodology for conducting impact assessments would be cognisant of freedom of sciences and scientific research.

Thirdly, the European Commission can, as a part of its science policy mandate gather evidence and request research on the rights and obligations stemming from EU (economic) regulation and their impact on scientific research. In this regard, there are some noteworthy developments with several studies already being commissioned that survey EU legislation on data and digital technologies, including AI, and that take the perspective of compliance by research performing organisations.⁴⁷⁰ Evidence on compliance issues and inconsistencies between different legal instruments which can negatively affect scientific research may help to calibrate EU law to better recognise the specific domain of scientific research. Moreover, the idea to introduce a regular monitoring exercise has its merits to keep tabs on the practical issues of complying with EU law in the context of scientific research, the internal coherence of EU legislation and the interfaces with private sector business models.

⁴⁷⁰ See: European Commission and Lundqvist 2022; European Commission and Angelopoulous 2022; European Commission and Senftleben 2022; and European Commission and Van Eechoud 2022. See also European Commission and PPMI et al 2024 (forthcoming).

Conclusions and recommendations

Rather than steering their own digital transformation, universities have played a largely reactive role in shaping the digital infrastructures and services that are nowadays used in academic research, educational programmes and institutional governance. Commercial digital suppliers have become a driving force in the digital design of public universities, which is increasingly shaped by the logic and values of the market. The ongoing commercialisation of the academic digital sphere bears the risk that the public values on which universities are founded might erode. Scientific advancement, academic freedom and institutional autonomy are important values that should be preserved and promoted moving forward with the digital transformation journey.

The objective of this report was to, firstly, break down the concept of digital sovereignty in the specific context of universities and scientific research, in such a way that it can be used by universities and academics to advance academic values, and their public missions more generally, in the digital age. Secondly, it aimed to give an account of the relevant regulations adopted under the EU's digital policies and determine their impact on universities' and academics' digital sovereignty. The two elements are reflected in the following research question: "*What does digital sovereignty mean within the university and scientific research context, how can it be leveraged to defend and promote academic values, and what is the role of EU law in this regard?*" Addressing this question, the report specifically focused on research activities oriented toward scientific advancement in the public interest; the branches of education and institutional governance were discussed where necessary.

Findings on digital sovereignty in the university context

Within the spectrum of digital sovereignty narratives, in the university and scientific research context the concept of "digital sovereignty" is intricately linked to universities' unique position in society and the specific values they embody and adhere to. **Chapter 1** concluded that both universities (as institutions) and academics (individually or collectively) can make 'claims' for digital sovereignty in relation to the design and governance of digital technologies and infrastructures as well as to the data residing in those digital infrastructures. Universities' and academics' digital sovereignty claims arise from, and are defined by, perceived *threats to academic values* correlated with the commercial supply of digital technologies and infrastructures that affect their ability to take autonomous decisions and actions regarding digital infrastructures and data.

As explained in **Chapter 2**, the quest for digital sovereignty by universities is primarily motivated by the need to protect fundamental academic values and, ultimately, uphold universities' public function as autonomous knowledge producers in the digital age. This report identified three 'core' values that have traditionally guided universities' commitments and activities: scientific advancement, individual academic freedom and institutional autonomy. Digital sovereignty can be framed as an *instrument* to defend and promote these values where their substance is threatened by certain dynamics of the digital transformation (see below).

As it followed from **Chapter 3**, universities are facing multiple threats to academic values, which give rise to various digital sovereignty claims. The threats – a non-exhaustive list of which has been compiled from literature – can be categorised as 'relating to digital technologies and infrastructures' and 'relating to data' respectively. With regard to digital infrastructures, the main threats include a concentration of relevant markets and the risk of technology-and-vendor lock ins; the bundling of read-and-publish services and data analytics services; and the external influence on independent research, education and institutional decision-making via techno-commercial architectures. On the data side, it is predominantly the value capture from user data, the lack of researchers' access to data held by commercial technology providers, and the instrumentalisation of publicly-funded research data for commercial purposes that,

amongst others, underpin claims for digital sovereignty. While universities have actively been taking measures to address these challenges, when confronted with sizeable information and power asymmetries, their capacity to assert digital sovereignty may not be large enough and arguably requires concerted strategies and regulatory backing.

Chapter 4 surveyed (recent) EU legislative action in the field of data, digital technologies and AI, which has produced both rights and obligations for universities and academics carrying out scientific research. Importantly, although European universities fully support the overarching policy objective of open science, the obligation to (openly) share research data does incur a new type of ‘overhead expenses’ weighing heavily on them. The overall picture that emerges when looking across EU digital and data legislation is that the piecemeal recognition of scientific research in EU regulation is rather incoherent and makes legal compliance for universities unnecessarily complex.

Based on the findings set out above, this report arrives at the following recommendations addressed to respectively universities and academics, EU law- and policymakers and research funding organisations.

Recommendations for universities and academics

As a basic premise, universities should (re-)claim agency over their digital design in order to (re)align their digital transformation with academic values. For universities and academics, formulating digital sovereignty claims is a first step to address the perceived threats to academic values. This report gathered experiences and strategies which have already proven successful in tackling digital sovereignty claims in the university context. In addition, it recommends to, *firstly*, ground academic values into university’s procurement framework; *secondly*, produce shared resources and for universities to team-up as a sector; and *thirdly*, selectively promote public interest-oriented digital technologies.

Develop a procurement framework based on academic values

The instances when universities contract third-party digital services and infrastructures are important opportunities to realise their digital sovereignty claims. In these situations, the goal of universities should be to look beyond monetary and utility attributes, and ensure that in the procurement from commercial suppliers academic values are fully respected. It is therefore necessary that universities have a framework for procurement in place in which commercial digital services and infrastructures and their potential impact on academic freedom and institutional autonomy are critically assessed, for instance by:

- Making **lock-in risk assessments** a part of procurement policy, in which the concentration of supplier markets is considered, and alternative product and service providers (including open source alternatives) as well as barriers to switching are carefully mapped out. It is imperative that universities select suppliers on the basis of a longer-term perspective to hidden costs and possible negative effects of the service beyond price.
- Making **data protection impact assessments** a part of procurement policy, considering in particular the risks stemming from personal data being processed for suppliers’ own purposes. Based on these assessments, universities can propose appropriate conditions on personal data to be incorporated in the service contract. They can also use the legal requirements of the General Data Protection Regulation as a backstop in contractual negotiations.
- Requiring **mandatory compliance audits** of providers of digital infrastructures and services, in regular intervals, so that suppliers have to demonstrate adherence to their contractual obligations and hold them accountable in case they fail to do so.

At the same time, universities must be aware that the use of certain digital tools may affect the individual academic freedom of researchers and teachers. They should therefore not unnecessarily restrict individual academics' ability to choose alternative tools, even though they have a portfolio of centrally procured tools at their disposal.

Produce shared knowledge and team-up as a sector

Universities should share knowledge about legal and technical assessments of frequently procured digital services and infrastructures. Moreover, they should (continue to⁴⁷¹) work together to increase their negotiation and bargaining power vis-à-vis powerful suppliers of digital services and infrastructures.

- **Producing shared knowledge** will reduce the burden of *individual* universities to carry out legal and technical assessments of suppliers of standard digital services and infrastructures. As documented in the Expert Memo, umbrella procedures can be harnessed for data protection impact assessments and compliance audits to the benefit of the whole university sector. Resulting documentation should be published and widely shared within the European Research Area.
- **Approaching negotiations and procurement collectively** – where appropriate – will scale up universities' bargaining power. Here, university associations and other organisations representing the university sector can assume the role of coordinators and devise sector-wide procurement frameworks that safeguard universities' digital sovereignty. Within the collaborative processes, it can be useful to establish 'specialisations' and 'leads' so that individual universities can oversee a portfolio while drawing from shared expertise.
- In the context of public procurement, **working together with the public sector** can also be a means to tackling universities' digital sovereignty claims. Since many universities (at least in the Netherlands) are organised as public sector bodies and to some extent deal with the same problems as other public sector bodies, they could benefit from being covered by wider public sector procurement frameworks that are non-negotiable for commercial suppliers.

Promote public interest oriented digital technologies

Importantly, universities' measures to (re)claim digital sovereignty should not be limited to 'taming' technology providers when procuring *commercial* digital infrastructures and services. Indeed, universities are also incubators and users of *public interest-oriented* technologies which uphold academic values as well. This report showed that the extent to which universities outsource cloud-based services to commercial suppliers varies significantly across Europe, which means that universities tend to assess the value of public digital infrastructures differently. This, in turn, means that public interest-oriented technologies are worth exploring as viable alternatives or additions to commercially supplied digital technologies, and as a strategy to diversify the digital portfolio of universities where appropriate.

Recommendations for law- and policymakers

The realisation of the European Research Area has a significant digital dimension, with the EU's Open Science Policy mandating the sharing of research data and implementing a European Open Science Cloud

⁴⁷¹ Dutch universities already have experience with joint IT procurement, for example via SURF, a collaborative organisation for ICT in Dutch higher education and research, see <<https://www.surf.nl/en/it-procurement-purchasing-it-together-at-the-best-possible-terms>>.

(EOSC). Moreover, legislation adopted under the EU's general digital strategy is increasingly shaping the legal landscape in which universities operate and carry out scientific research. It follows from this report that there is a need for better recognition of scientific freedom; consolidation of the notion of scientific research; and strengthening of internal consistency between the various legislative instruments of EU digital and data law. Law- and policymakers are advised to:

- **Give broad recognition to scientific freedom as a cross-cutting policy issue** that transcends the EU's Open Science Policy and elevates the objectives of scientific research throughout the EU's policy cycle. An increased focus on scientific research can contribute to ensuring a fair and inclusive digital transformation for universities. Relatedly, law- and policymakers are encouraged to develop a vision and strategy on researchers' access to externally-held data that are necessary to perform research and understand our contemporary society.
- **Adopt a consistent notion and definition of scientific research across legislation** which emphasises the public-interest nature of scientific research and its adherence to recognised ethical standards of scientific research and open science. Where appropriate, a distinction should be made between commercial and public-interest driven scientific research when it comes to granting legal privileges and exceptions.
- **Continually assess and address the coherence of EU legislation** from the perspective of scientific freedom and promoting scientific research. As far as EU digital and data regulation is concerned, scientific research is not consistently recognised, which has made universities' and academics' compliance with legal obligations and recourse to rights unnecessarily complex.

Recommendations for research funding organisations

Finally, research funding organisations, both at EU and Member State level, have the financial means to **support the development** by universities of **public interest-oriented technologies and public digital infrastructures** as alternatives or additions to commercial infrastructures and services. Moreover, research funding organisations can relieve the burden imposed on universities to make publicly-funded research data available for re-use – which are a new type of 'overhead expenses' – by **funding the management and sharing of research data** while avoiding that this funding eats into the funding of actual research activities.⁴⁷²

In conclusion, the articulation of digital sovereignty claims by universities and academics can become a useful framing in order to set in motion a more proactive strategy to defend and preserve academic values when outsourcing digital infrastructures and services to commercial suppliers. An important venue for putting the freedom of sciences and the right to research centre stage is EU law and policy, which exercises increasing influence on the conditions under which universities and academics carry out public interest-oriented scientific research

⁴⁷² Meaning that research funding must be increased accordingly to reflect the full cost of making research data available, see also Sorbonne declaration 2020, p. 2.

Bibliography

Introduction

Literature

Constantinides, Henfridsson and Parker 2018

P. Constantinides, O. Henfridsson, G.G. Parker, 'Introduction – Platforms and Infrastructures in the Digital Age', *Information Systems Research*, Vol. 29, No. 2, pp. 381-400.

Digitale Agenda UvA 2022

Universiteit van Amsterdam, 'Digitale Agenda UvA [Beleidsdocument]', 25 May 2022. Available at: <https://www.uva.nl/over-de-uva/beleid-en-regelingen/algemeen/digitale-agenda.html>.

Ferrari 2023

V. Ferrari, *Money after Money: disassembling value/ information infrastructures*, (diss. Amsterdam UvA) 2023.

Henfridsson and Bygstad 2023

O. Henfridsson and B. Bygstad, 'The Generative Mechanisms of Digital Infrastructure Evolution', *MIS Quarterly* 2013, Vol. 37, No. 3, pp. 907-932.

Institute for Information Law 2023b

Institute for Information Law, 'Information Law and the Digital Transformation of the University: Digital Sovereignty, Data Governance and Researchers' Access to Data – Part II. Access to Data for Research', 2023 <https://www.ivir.nl/part-ii-access-to-data-for-research/>.

LERU Data Statement 2021

LERU, 'LERU Data Statement', 2021. Available at: <https://www.leru.org/publications/is-university-autonomy-threatened-by-eu-data-policy-and-law>.

Maex 2021

K. Maex, 'Protect independent and public knowledge', *Lecture at the Dies Natalis of the University of Amsterdam*, 10 January 2021. Available at: https://uva.uas.figshare.com/articles/presentation/Digital_University_Act_pdf/13553825.

Maex et al 2019

K. Maex et al, 'Digitalisering bedreigt onze universiteit. Het is tijd om een grens te trekken', *de Volkskrant* 22 December 2019.

Roosendaal 2023

A. Roosendaal, 'The GDPR as a means to protect digital sovereignty of universities' (Expert Memo), 2023 <https://www.ivir.nl/expert-memo>.

SURF Strategy 2022-2027

SURF, '3 Roles 1 SURF: Strategy 2022-2027', 2022. Available at: <https://www.surf.nl/en/our-focus-for-2022-2027>.

Van Dijck, Nieborg and Poell 2019

J. van Dijck, D. Nieborg and T. Poell, 'Reframing platform power', *Internet Policy Review* 2019, Alexander von Humboldt Institute for Internet and Society, Vol. 8, No. 2.

Chapter 1

Legislation

Applicable and adopted

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), ELI:

<<http://data.europa.eu/eli/reg/2022/868/oj>>.

Regulation (EU) 2018/1807 of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, ELI: <<http://data.europa.eu/eli/reg/2018/1807/oj>>.

Legislative proposals

Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM/2022/68 final.

- Latest version: Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) – Mandate for negotiations with the European Parliament, 17 March 2023, 7413/23.

Policy documents

M. Von der Leyen, '2021 State of the Union Address'. Available at:

<https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_21_4701>.

European Commission, Staff Working Document Impact Assessment Report accompanying Proposal for a Regulation on European Data Governance (Data Governance Act), 12 November 2020, SWD(2020) 295 final.

European Commission, 'A European strategy for data', 19 February 2020, COM(2020) 66 final.

European Commission, Staff Working Document Impact Assessment Accompanying Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, 13 September 2017, SWD(2017) 304 final.

Literature

Amankwah-Amoah et al 2021

J. Amankwah-Amoah et al, 'COVID-19 and digitalization: The great acceleration', *Journal of Business Research*, 2021, 136, pp. 602-611.

Angeli et al 2022

L. Angeli et al, 'Conceptualising Resources-aware Higher Education Digital Infrastructure through Self-hosting: a Multi-disciplinary View', in: *Eight Workshop on Computing withing Limits*. Available at: <<https://computingwithinlimits.org/2022/papers/limits22-final-Angeli.pdf>>.

Aspesi et al 2019a (SPARC Landscape Analysis)

C. Aspesi et al, *Landscape Analysis: The Changing Academic Publishing Industry – Implications for Academic Institutions*, SPARC 2019. Available at: <<https://infrastructure.sparcopen.org/landscape-analysis>>.

Bendiek and Stürzer 2022

A. Bendiek and I. Stürzer, I., ‘Advancing European Internal and External Digital Sovereignty: The Brussels Effect and the EU-US Trade and Technology Council’, 2022, *Stiftung Wissenschaft und Politik* 2022/C 20. Available at: <<https://www.swp-berlin.org/en/publication/advancing-european-internal-and-external-digital-sovereignty>>.

Bok et al 2021 (VSNU)

C. Bok et al 2021, *Advies publieke waarden voor het onderwijs* (Werkgroep publieke waarden), Den Haag: VSNU 2021. Available at: <<https://www.universiteitenvannederland.nl/2020/publieke-waarden-en-academische-soevereiniteit.html>>.

Seifried et al 2021

M. Seifried et al, *Schwerpunktstudie Digitale Souveränität – Bestandaufnahme und Handlungsfelder*, Berlin: Bundesministerium für Wirtschaft und Energie (BMWi) 2021. Available at: <<https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/schwerpunktstudie-digitale-souveranitaet.html>>.

Calzada 2021

I. Calzada, ‘Data Co-Operatives through Data Sovereignty’, *Smart Cities* 2021, Vol. 4, pp. 1158–1172.

Christakis 2020

T. Christakis, “‘European Digital Sovereignty’: Successfully Navigating Between the “Brussels Effect” and Europe’s Quest for Strategic Autonomy’, Multidisciplinary Institute on Artificial Intelligence/Grenoble Alpes Data Institute, e-book, December 2020. Available at: <<https://ai-regulation.com/articles/#>>.

DFG Briefing Paper 2021

Committee on Scientific Library Services and Information Systems of the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation), *Data tracking in research: aggregation and use or sale of usage data by academic publishers* (Briefing paper), 28 October 2021. Available at: <https://www.dfg.de/download/pdf/foerderung/programme/lis/datentracking_papier_en.pdf>.

Desmarais-Tremblay 2020

M. Desmarais-Tremblay, ‘W.H. Hutt and the conceptualization of consumers’ sovereignty’, *Oxford Economic Papers* 2020, Vol. 72, No. 4, pp. 1050-1071.

EIT Digital 2020

EIT Digital, *European Digital Infrastructure and Data Sovereignty: A Policy Perspective*. Brussels: EIT Digital 2020. Available at: <<https://eit.europa.eu/sites/default/files/eit-digital-data-sovereignty-full-report.pdf>>.

Fiebig et al 2023

T. Fiebig et al, ‘Heads in the Clouds? Measuring Universities’ Migration to Public Clouds: Implications for Privacy & Academic Freedom’, *Proceedings on Privacy Enhancing Technologies* 2023(2). Available at <https://pure.mpg.de/rest/items/item_3480830_3/component/file_3482426/content>.

Fiebig and Aschenbrenner 2022

T. Fiebig and D. Aschenbrenner, ‘13 Propositions on an Internet for a “Burning World”’, *TAURIN+BGI '22: Proceedings of the ACM SIGCOMM Joint Workshops on Technologies, Applications, and Uses of a Responsible Internet and Building Greener Internet*, August 2022, Amsterdam. Netherlands. Available at: <https://pure.mpg.de/rest/items/item_3390006_3/component/file_3456420/content>.

Floridi 2020

L. Floridi, 'The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU', *Philosophy & Technology* 2020, Vol. 33, No. 3, pp. 369–378.

German Federal Institute for Research on Building, Urban Affairs and Spatial Development 2021

German Federal Institute for Research on Building, Urban Affairs and Spatial Development (BBSR) within the Federal Office for Building and Regional Planning (BBR), *Data strategies for common good-oriented urban development*, October 2021. Available at: <<https://www.smart-city-dialog.de/wp-content/uploads/2021/12/data-strategies-common-urban-development-dl-1.pdf>>.

German Federal Ministry for Economic Affairs and Energy 2019

German Federal Ministry for Economic Affairs and Energy, *Project GALA-X: A Federated Data Infrastructure as the Cradle for a Vibrant European Ecosystem*, October 2019. Available at: <https://www.data-infrastructure.eu/GAIA-X/Redaktion/EN/Publications/project-gaia-x.pdf?__blob=publicationFile&v=5>.

Goldenfein and Griffin 2022

J. Goldenfein and D. Griffin, 'Google Scholar – Platforming the scholarly economy', *Internet Policy Review* 2022, Vol. 11, No. 3.

Grevi 2019

G. Grevi, *Strategic autonomy for European choices: The key to Europe's shaping power* (Discussion Paper), European Policy Centre 2019. Available at: <<https://www.epc.eu/en/publications/Strategic-autonomy-for-European-choices-The-key-to-Europes-shaping-p~213400>>.

Haché 2017

A. Haché, 'Technological Sovereignty: Learning to love machines again', in: M. Padilla (Ed.), *Technological Sovereignty Vol. 2*, Barcelona: Descontrol 2017, pp. 17-29. Available at : <<https://www.ritimo.org/IMG/pdf/sobtech2-en-with-covers-web-150dpi-2018-01-10.pdf>>.

Irion 2022

K. Irion, 'The General Data Protection Regulation through the lens of digital sovereignty', in: D. Broeders (Ed.), *Digital Sovereignty: From Narrative To Policy?* (Report EU Cyber Direct – EU Cyber Diplomacy Initiative project), 2022, pp. 53-57. Available at: <<https://eucyberdirect.eu/research/digital-sovereignty-narrative-policy>>

Irion 2013

K. Irion, 'Government Cloud Computing and National Data Sovereignty', *Policy & Internet* 2013, Vol. 4, No. 3-4, pp. 40-71.

Kitchin 2018

R. Kitchin, 'Reframing, Reimagining and Remaking Smart Cities', in : C. Coletta et al (Eds.), *Creating Smart Cities*, Routledge: London 2018, pp. 219-230. Contribution available at: <<https://kitchin.org/wp-content/uploads/2020/02/Creating-smart-cities-chapter-17-2018.pdf>>.

KNAW 2022

Koninklijke Akademie van Wetenschappen (KNAW, Royal Netherlands Academy of Arts and Science), *The pandemic academic. How COVID-19 has impacted the research community*, Amsterdam 2022. Available at: <<https://www.knaw.nl/publicaties/pandemic-academic-how-covid-19-has-impacted-research-community>>.

Lambach and Oppermann 2022

D. Lambach and K. Oppermann, 'Narratives of digital sovereignty in German political discourse', *Governance* 2022, pp. 1-17.

Leonard and Shapiro 2019

M. Leonard and J. Shapiro, *Empowering EU Member States with Strategic Sovereignty*, European Council on Foreign Relations 2019. Available at:

<https://ecfr.eu/publication/strategic_sovereignty_how_europe_can_regain_the_capacity_to_act/>.

Madiega (European Parliamentary Research Service) 2020

T. Madiega, *Digital sovereignty for Europe* (Briefing paper), Brussels: European Parliamentary Research Service 2020. Available at:

<[https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf)>.

Maex et al 2019

K. Maex et al, 'Digitalisering bedreigt onze universiteit. Het is tijd om een grens te trekken', *Volkskrant* 22 December 2019.

Mayer-Schönberger 2020

V. Mayer-Schönberger, 'Regulation the Feedback Effect', in: K. Werbach (Ed.), *After the Digital Tornado: Networks, Algorithms, Humanity*, Cambridge: Cambridge University Press 2020, pp. 122-136.

Moerel and Timmers 2020

L. Moerel and P. Timmers, *Reflecties over digitale soevereiniteit*, Preadvies Staatsrechtconferentie 2020. Available at:

<<https://www.uu.nl/agenda/staatsrechtconferentie-staatsrecht-in-de-datasamenleving>>.

Morozov and Bria 2018

E. Morozov and F. Bria, *Rethinking the smart city: Democratizing urban technology*, New York: Rosa Luxemburg Foundation 2018. Available at: <<https://rosalux.nyc/rethinking-the-smart-city/>>.

Nicholds and Garcia 2022

T.P. Nicholds and A. Garcia, 'Platform Studies in Education', *Harvard Educational Review* 2022, Vol. 92, No. 2, pp. 209–230.

Padilla 2017

M. Padilla, *Technological Sovereignty Vol. 2*, Barcelona: Descontrol 2017. Available at:

<<https://www.ritimo.org/IMG/pdf/sobtech2-en-with-covers-web-150dpi-2018-01-10.pdf>>.

Poell, Nieborg and Van Dijck 2019

T. Poell, N. Nieborg and J. Van Dijck, 'Platformisation', *Internet Policy Review* 2019, Vol. 8, No. 4.

Pohle 2020

J. Pohle, *Digital sovereignty. A new key concept of digital policy in Germany and Europe*, Berlin: Konrad-Adenauer-Stiftung 2020. Available at: <<https://www.econstor.eu/bitstream/10419/228713/1/Full-text-report-Pohle-Digital-sovereignty.pdf>>.

Pohle and Thiel 2020

J. Pohle and T. Thiel, 'Digital sovereignty', *Internet Policy Review* 2020, Vol 9, No. 4.

Riemens 2014

P. Riemens, 'Technological Sovereignty: a Necessity and a Challenge', in: S. Couture et al (Eds.), *For Free Information and Open Internet: Independent journalists, community media and hacktivists take action*, Paris: Passerelle Collection by Ritimo, No. 11 2014. Available at <<https://www.coredem.info/rubrique48.html>>.

Roberts et al 2021

H. Roberts et al, 'Safeguarding European values with digital sovereignty: an analysis of statements and policies', *Internet Policy Review* 2021, Vol. 10, No. 3.

Sharon 2021

T. Sharon, 'Blind-sided by privacy? Digital contract tracing, the Apple/Google API and big tech's newfound role as global health policy makers', *Ethics and Information Technology* 2021, Vol. 23, Suppl. 1, pp. 545-557.

Schulz et al 2022

E. Schultz et al, *Digitale Souveränität: Von der Hochschulbildung für die Forschung* (Discussion Paper of the Working Group "Digitales Lernen, Lehren und Vernetzen" within the Priority Initiative "Digitale Information" of the Alliance of German Science Organisations), 2022. Available at: <https://gfzpublic.gfz-potsdam.de/rest/items/item_5013059_2/component/file_5013060/content>.

Soare 2022

S.R. Soare, in: D. Broeders (Ed.), *Digital Sovereignty: From Narrative To Policy?* (Report EU Cyber Direct – EU Cyber Diplomacy Initiative project), 2022, pp. 19-24. Available at: <<https://eucyberdirect.eu/research/digital-sovereignty-narrative-policy>>.

Stolwijk et al 2022

C. Stolwijk et al, *Bridging the Dutch and European Digital Sovereignty gap*, Den Haag: TNO 2022. Available at: <<https://www.tno.nl/en/newsroom/insights/2022/06/strengthening-digital-sovereignty-makes/>>.

Timmers 2019

P. Timmers, 'Ethics of AI and Cybersecurity When Sovereignty is at Stake', *Minds and Machines* 2019, Vol. 29, pp. 635-645.

Ozalp et al 2022

H. Ozalp et al, "'Digital Colonization" of Highly Regulated Industries: An Analysis of Big Tech Platforms' Entry into Health Care and Education', *California Management Review* 2022, Vol. 64, No. 4, pp. 78-107.

Persky 1993

J. Persky, 'Consumer Sovereignty', *Journal of Economic Perspectives* 1993, Vol. 7, No. 1.

Sellar and Hogan 2019

S. Sellar and A. Hogan, *Pearson 2025: Transforming teaching and privatizing education data*, Brussels: Education International 2019. Available at: <<https://www.ei-ie.org/en/item/25681:pearson-2025-transforming-teaching-and-privatising-education-data>>.

Thieulin 2019

B. Thieulin, *Towards a European digital sovereignty policy* (Opinion of the French Economic, Social and Environmental Council), March 2019. Available at: <https://www.lecese.fr/sites/default/files/travaux_multilingue/2019_07_souverainete_europeenne_numerique_G_B_reduit.pdf>.

Vadiati 2022

N. Vadiati, 'Alternatives to smart cities: A call for consideration of grassroots digital urbanism', *Digital Geography and Society* 2022, Vol. 3.

Van Dijck, Poell and De Waal 2018

J. Van Dijck, T. Poell and M. de Waal, *The Platform Society: Public Values in a Connective World*, Oxford: Oxford University Press 2018.

Vleugels and Van Wijnen 2022

A. Vleugels and J.F. Van Wijnen, 'Studentgegevens ondanks kritiek massaal in cloud bij techgiganten', *Het Financieele Dagblad* 17 October 2022.

Walzer 1983

M. Walzer, *Spheres of justice: a defense of pluralism and equality*, Oxford: Robertson 1983.

Williamson 2021

B. Williamson, 'Making markets through digital platforms: Pearson, edu-business, and the (e)valuation of higher education', *Critical Studies in Education* 2021, Vol. 62, No. 1, pp. 50-66.

Williamson, Bayne and Shay 2020

B. Williamson, S. Bayne and S. Shay, 'The datafication of teaching in Higher Education: critical issues and perspectives', *Teaching in Higher Education* 2020, Vol. 25, No. 4, pp. 351-365.

Williamson and Hogan 2020

B. Williamson and A. Hogan, 'Commercialisation and privatisation in/of education in the context of Covid-19', Brussels: Education International 2020. Available at:

<https://issuu.com/educationinternational/docs/2020_eiresearch_gr_commercialisation_privatisation>.

Declarations and statements

Berlin Declaration on Digital Society and Value-Based Digital Government 2020

Berlin Declaration on Digital Society and Value-Based Digital Government, signed at the ministerial meeting during the German Presidency of the Council of the European Union on 8 December 2020. Available at:

<<https://www.bmi.bund.de/SharedDocs/pressemitteilungen/EN/2020/12/berlin-declaration-digitalization.html>>.

DSN Position Paper 2021

Data Sovereignty Now (DSN), *Stimulating the Digital Economy by introducing the Principle of "Data Sovereignty"* (Position Paper), 2021. Available at: <<https://datasovereignty.org/2021/02/23/position-paper-the-benefits-of-data-sovereignty/>>.

European Digital SME Alliance 2021

European Digital SME Alliance, *White Paper on Digital Sovereignty*, 27 October 2021. Available at :

<https://www.digitalsme.eu/digital/uploads/Position-paper-on-Digital-Sovereignty-White-Paper_FINAL-DRAFT.pdf>.

French and German Governments 2019

French and German Governments, *A Franco-German Manifesto for a European industrial policy fit for the 21st Century*, 19 February 2019. Available at: <<https://www.bmwk.de/Redaktion/DE/Downloads/F/franco-german-manifesto-for-a-european-industrial-policy.html>>.

Franco-German Position on Gaia-X 2020

Representatives of industries, cloud service providers and cloud services customers from France and Germany, *Franco-German Position on GALA-X*, 18 February 2020. Available at:

<https://www.bmwk.de/Redaktion/DE/Downloads/F/franco-german-position-on-gaia-x.pdf?__blob=publicationFile&v=10>.

Blogposts, webpages, videos, other

Ausloos, Toh and Giannopoulou 2022

J. Ausloos, J. Toh and A. Giannopoulou, 'The case for collective action against the harms of data-driven technologies', 23 November 2022, Ada Lovelace Institute, <<https://www.adalovelaceinstitute.org/blog/collective-action-harms/>>.

Belleman and Van Dijck 2022

B. Belleman and T. Van Dijck, 'Universities must take ICT and data into their own hands again', 21 January 2022, Delta, <<https://www.delta.tudelft.nl/article/universities-must-take-ict-and-data-their-own-hands-again>>.

Borell 2020

J. Borell, 'Why European strategic autonomy matters', 3 December 2020, European Union External Action, <https://www.ecas.europa.eu/ecas/why-european-strategic-autonomy-matters_en>.

Bria 2020

F. Bria, 'Putting tech and innovation at the service of people and the green transition', UCL IIPP Blog, 9 March 2020, <<https://medium.com/iipp-blog/putting-tech-and-innovation-at-the-service-of-people-and-the-green-transition-2e039ab8e083>>.

European Commission, 'A Europe Fit for the Digital Age' (webpage)

European Commission, 'A Europe Fit for the Digital Age' (webpage), <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en>.

European Commission, 'Europe: the Keys to Sovereignty' (news webpage)

European Commission, 'Europe: the Keys to Sovereignty' (news webpage), <https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en>.

Hogan 2018

A. Hogan, 'Marketisation, privatisation & commercialisation in education: defining key terms', 12 December 2018, Education International, <<https://www.ei-ie.org/en/item/26108:marketisation-privatisation-commercialisation-in-education-defining-key-terms>>.

Jansen 2021

D. Jansen, 'Safeguarding academic and digital sovereignty: a model for action', 19 October 2021, European University Association, <<https://eua.eu/resources/expert-voices/250:safeguarding-academic-and-digital-sovereignty-a-model-for-action.html>>.

Michel 2021

C. Michel, 'Digital sovereignty is central to European strategic autonomy' – Speech by President Charles Michel at "Masters of digital 2021" online event, 3 February 2021, European Council, <<https://www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digitaleurope-masters-of-digital-online-event/>>.

Microsoft Customer Stories 2021

Microsoft Customer Stories, 'Nyenrode Business University: Connecting data sources in a unified way', 27 April 2021, Microsoft, <<https://customers.microsoft.com/en-us/story/1360699875743841506-nyenrode-business-university-higher-education-azure-en-netherlands>>.

Online Sphere Transgression Watch digital tool

iHub, Sphere Transgression Watch digital tool, <<https://ihub.ru.nl/news/post.page?id=3lwqJ3v0M0b>>.

Sanders 2012

R. Sanders, 'Amerikaanse Caci koopt PSB Informatiesystemen', 30 May 2012, Computable, <<https://www.computable.nl/artikel/nieuws/erp/4524822/250449/amerikaanse-caci-koopt-psb-informatiesystemen.html>>.

Smart City Dialog, 'Data Sovereignty: a key issue for municipalities'

Smart City Dialog, 'Data Sovereignty: a key issue for municipalities. Available at <<https://www.smart-city-dialog.de/en/news/data-sovereignty-a-key-issue-for-municipalities-2>>.

Sharon at the PublicSpaces Conference 2022 (video)

'Tamar Sharon: Sphere Transgression by Tech Giants', PublicSpaces Conference 2022 (video), <<https://conference.publicspaces.net/en/session/keynote-bu>>.

Van Gaal 2019

J. van Gaal, 'ID first department to completely switch to Office 365', 2 July 2019, Cursor, <<https://www.cursor.tue.nl/en/news/2019/juli/week-1/id-first-department-to-completely-switch-to-office-365/>>.

Van Santen (SURF) 2022

W. Van Santen (SURF), 'UPDATE: Videobellen: snel, simpel en veilig', 9 May 2022, SURF, <<https://communities.surf.nl/artikel/update-videobellen-snel-simpel-en-veilig>>.

Fleming 2021

S. Fleming, 'What is digital sovereignty and why is Europe so interested in it?', 15 March 2021, World Economic Forum, <<https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/>>.

Chapter 2

Legislation

International

Conventions

United Nations (General Assembly), Universal Declaration of Human Rights (UDHR), 10 December 1948, 217 A (III).

United Nations (General Assembly), International Covenant on Economic, Social and Cultural Rights (ICESCR), Treaty Series, 16 December 1966, Treaty Series, Vol. 993.

Soft law

General Comment No. 25 of the Committee on Economic, Social and Cultural Rights (CESCR) (30 April 2020), *On science and economic, social and cultural rights (article 15(1)(b), (2), (3) and (4) of the International Covenant on Economic, Social and Cultural Rights)*.

General Comment No. 13 of the Committee on Economic, Social and Cultural Rights (CESCR) (8 December 1999), *The Right to Education (Art. 13)*.

Recommendation concerning the Status of Higher-Education Teaching Personnel of the United Nations Educational, Scientific and Cultural Organization (UNESCO), 1997.

Revised Recommendation on Science and Scientific Researchers of the United Nations Educational, Scientific and Cultural Organization (UNESCO), adopted during the 39th session of the General Conference in Paris, 30 October-14 November 2017. See Records of the 39th session of the General Conference, Annex II. Available at: <<https://unesdoc.unesco.org/ark:/48223/pf0000260889.page=116>>.

United Nations, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (David Kaye), A/HRC/29/32, 2015: *Report on encryption, anonymity, and the human rights framework*. Available at: <<https://www.ohchr.org/en/documents/thematic-reports/ahrc2932-report-encryption-anonymity-and-human-rights-framework>>.

United Nations, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (David Kaye), Note by the Secretary-General, A/75/261, 2020: *Report on academic freedom and the freedom of opinion and expression*. Available at: <<https://www.ohchr.org/en/documents/thematic-reports/a75261-report-academic-freedom-and-freedom-opinion-and-expression>>.

Council of Europe

Conventions

Council of Europe, European Convention on Human Rights (ECHR), as amended by Protocols Nos. 11, 14 and 15 and supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16.

Soft law

Resolution 2352 of the Parliamentary Assembly of the Council of Europe (20 November 2020), *Threats to academic freedom and autonomy of higher education institutions in Europe*.

Recommendation CM/Rec(2012)7 of the Committee of Ministers of the Council of Europe (20 June 2012), *On the responsibility of public authorities for academic freedom and institutional autonomy*.

Recommendation CM/Rec (2007)6 of the Committee of Ministers of the Council of Europe (16 May 2007), *On the public responsibility for higher education and research*.

Recommendation 1762(2006) of the Parliamentary Assembly of the Council of Europe (30 June 2006), *Academic Freedom and University Autonomy*.

Recommendation R(2000)8 of the Committee of Ministers of the Council of Europe (30 March 2000), *On the research mission of universities*.

European Union

Primary EU Law

Charter of Fundamental Rights of the European Union (CFREU), *OJ EU* 2012, C 326/391.

Directives and regulations

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directive 96/9/EC and 2001/29/EC (CDSM Directive).

Soft law

Explanations Relation to the Charter of Fundamental Rights, 2007/C 303/02.

Recommendation of the European Parliament, *On defence of academic freedom in the EU's external action* (2018/2117(INI)), 29 November 2018.

Preliminary Opinion of the European Data Protection Supervisor (EDPS), *On data protection and scientific research*, 6 January 2020.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *On a European strategy for universities* (COM(2022) 16 final), 18 January 2022.

The Netherlands

Dutch Law on Higher Education and Scientific Research (*Wet op het hoger onderwijs en wetenschappelijk onderzoek*).

Kamerstukken II, 1990-1991, 21 073, nr. 17 (Wet op het hoger onderwijs en wetenschappelijk onderzoek; Vierde nota van wijziging).

Kamerstukken II, 1980-1981, 16 802, nr. 3 (Wet op het wetenschappelijk onderwijs 1981; Memorie van Toelichting).

Other

Annex I of the Rome Ministerial Communiqué of the Ministers responsible for Higher Education, adopted during the European Higher Education Area (EHEA) Ministerial Conference 2020. Available at: http://www.ehea.info/Upload/Rome_Ministerial_Communique_Annex_I.pdf.

Spanish Organic Law 6/2001 on Universities (*Ley Orgánica 6/20,01, de 21 de diciembre, de Universidades*). Available at: <https://www.global-regulation.com/translation/spain/1451484/law-6-2001%252c-of-21-december%252c-on-universities.html>.

Declarations and statements

Abidjan Principles 2019

Abidjan Principles (2019). Guiding Principles on the human rights obligations of States to provide public education and to regulate private involvement in education.

Association of American Universities 2013

Association of American Universities (AAU) (2013). Academic Principles: A Brief Introduction.

American Association of University Professors (AAUP) 1940

American Association of University Professors (AAUP), 1940 Statement of Principles on Academic Freedom and Tenure with 1970 Interpretive Comments.

American Association of University Professors (AAUP) 1915

American Association of University Professors (AAUP), 1915 Declaration of Principles on Academic Freedom and Academic Tenure.

Bonn Declaration 2020

Bonn Declaration on Freedom of Scientific Research (2020).

Dar es Salaam Declaration 1990

Dar es Salaam Declaration on Academic Freedom and Social Responsibility of Academics (1990).

European University Association (EUA) Lisbon Declaration 2007

European University Association (EUA) Lisbon Declaration (2007).

Declaration adopted at the Global Forum on Academic Freedom, Institutional Autonomy and the Future of Democracy 2019

Declaration adopted at the Global Forum on Academic Freedom, Institutional Autonomy, and the Future of Democracy (2019).

International Association of Universities (IAU) policy statement 1998

International Association of Universities (1998). Policy Statement on Academic Freedom, University Autonomy and Social Responsibility.

Leiden Principles 2022

Leiden Principles: The role of research-intensive universities as the world emerges from the COVID-19 pandemic.

Magna Charta Universitatum 1988

Magna Charta Universitatum (1988).

Magna Charta Universitatum 2020

Magna Charta Universitatum (2020).

Sorbonne declaration 2020

Sorbonne declaration on research data rights (2020).

World University Service Lima Declaration 1988

World University Service (1988). The Lima Declaration on Academic Freedom and Autonomy of Institutions of Higher Education.

Case law**Court of Justice of the European Union**

ECJEU 6 October 2020, C-66/18 (*European Commission v. Hungary*), ECLI:EU:C:2020:792.

Opinion of Advocate General Mengozzi in case C-15/13, 8 May 2014 (*Technische Universität Hamburg-Harburg v. Datenlotsen Informationssysteme GmbH*), ECLI:EU:C:2014:23.

Opinion of Advocate General Kokott in case C-66/18, 5 March 2020 (*Commission v. Hungary*), ECLI:EU:C:2020:172.

European Court of Human Rights

ECtHR 27 May 2014, App. Nos. 3346/04 and 3977/04 (*Mustafa Erdogan and Others v. Turkey*).

ECtHR 15 April 2014, App. No. 40877/07 (*Hasan Yazici v. Turkey*).

ECtHR 15 March 2012, App. Nos. 4149/04 and 41029/04 (*Aksu v. Turkey*).

ECtHR 23 June 2009, App. No. 17089/03 (*Sorguc v. Turkey*).

ECtHR 20 October 2009, App. No. 39128/05 (*Lombardi Vallauri v. Italy*).

ECtHR 22 May 1990, App. No. 12726/87 (*Autronic AG v. Switzerland*).

The Netherlands

CRvB 19 January 2019, ECLI:NL:CRVB:2018:51.

CRvB 5 February 2015, ECLI:NL:CRVB:2015:285.

Rb Noord-Holland 2 November 2017, ECLI:NL:RBNHO:2017:9139.

Other

U.S. Supreme Court, *University of Michigan v. Ewing*, 474 U.S. 214 (1985).

Literature

Altbach 2001

P.G. Altbach, 'Academic freedom: International realities and challenges', *Higher Education* 2001, Vol. 41, No. 1, pp. 205-2019.

ARTICLE 19 Policy Brief 2017

ARTICLE 19, *The Global Principles on Protection of Expression and Privacy* (Policy Brief), 2017. Available at:

<<https://www.article19.org/data/files/medialibrary/38657/Expression-and-Privacy-Principles-1.pdf>>.

Aspesi et al (SPARC) 2019b

C. Aspesi, et al, *A Roadmap for Action: Academic Community Control of Data Infrastructure*, Lincoln, Nebraska, USA:

University of Nebraska 2019. Available at: <<https://digitalcommons.unl.edu/scholcom/130/>>.

Beaud 2022

O. Beaud, 'Academic Freedom in France: A Concept Neglected and Liberties under Threat', in: De Gennaro, I., Hofmeister, H. and Lüfter, R. (Eds), *Academic Freedom in the European Context: Legal, Philosophical and Institutional Perspectives*, Cham: Palgrave MacMillan 2022, pp. 205-241.

Bennetot Pruvot, Estermann and Popkhadze 2023

E. Bennetot Pruvot, T. Estermann and N. Popkhadze, *University Autonomy in Europe IV: The Scorecard 2023*, European University Association (EUA) 2023. Available at: <<https://www.eua.eu/resources/publications/1061:university-autonomy-in-europe-iv-the-scorecard-2023.html>>.

Berlin 1969

I. Berlin, 'Two concepts of liberty', in: I. Berlin, *Four Essays on Liberty*, Oxford University Press 1969. Essay available at: <<http://faculty.www.umb.edu/steven.levine/Courses/Action/Berlin.pdf>>.

Bergan and Harkavy 2020

S. Bergan and I. Harkavy, 'Academic freedom, institutional autonomy and the engaged university', S. Bergan, T. Gallagher and I. Harkavy, *Academic Freedom, Institutional Autonomy and the Future of Democracy*, Council of Europe Higher Education Series No. 24, Strasbourg: Council of Europe Publishing 2020, pp. 15-28.

Bergan, Noorda and Egron-Polak 2020

S. Bergan, S. Noorda and E. Egron-Polak, 'Academic freedom and institutional autonomy – What role in and for the EHEA?', in: S. Bergan, T. Gallagher and I. Harkavy, *Academic Freedom, Institutional Autonomy and the Future of Democracy*, Council of Europe Higher Education Series No. 24, Strasbourg: Council of Europe Publishing 2020, pp. 41-55.

Deca 2020

L. Deca, 'Institutional autonomy and academic freedom: the complex role of public authorities', in: S. Bergan, T. Gallagher and I. Harkavy, *Academic Freedom, Institutional Autonomy and the Future of Democracy*, Council of Europe Higher Education Series No. 24, Strasbourg: Council of Europe Publishing 2020, pp. 155-162.

De Cock and Timbermont 2021

W. De Cock and E. Timbermont, 'Hof van Justitie kiest voor brede benadering van het concept 'academische vrijheid', zaak C-66/18, Commissie/Hongarije', *SEW, Tijdschrift voor Europees en economisch recht* 2021, Vol. 7/8 (July/August), Nr. 1. Available at: <<https://www.uitgeverijparis.nl/nl/reader/209911/1001584994#voetnoot43>>.

Finkin and Post 2009

M.W. Finkin and R.C. Post, *For the Common Good: Principles of American Academic Freedom*, New Haven: Yale University Press 2009.

GPPI 2021

Global Public Policy Institute (GPPI), 'Free Universities: Putting the Academic Freedom Index Into Action', available at: <https://gppi.net/media/KinzelbachEtAl_2021_Free_Universities_AFi-2020_upd.pdf>.

De Groof 2010

J. de Groof, 'Omtrent de academische vrijheid. Het 'Palladium' van de Universiteit?', in: Fleerackers, F. and Van Ransbeek, R. (Eds.), *Recht en onafhankelijkheid. De onafhankelijkheid van de rechtswetenschap*, Brussel: Larcier 2010, pp. 5-90.

Häyrynen-Alestalo and Peltola 2006

M. Häyrynen-Alestalo and U. Peltola, 'The problem of a market-oriented university', *Higher Education* 2006, Vol. 52.

Hofstadter and Metzger 1955

R. Hofstadter and W.P. Metzger, *The development of academic freedom in the United States*, New York: Columbia University Press 1955.

Horwitz 2005

P. Horwitz, 'Grutter's First Amendment', *Boston College Law Review* 2005, Vol. 46, pp. 461-590.

Karran 2009a

T. Karran, 'Academic freedom: in justification of a universal ideal', *Studies in Higher Education* 2009, Vol. 34, No., 3, pp. 265-268.

Karran 2009b

T. Karran, 'Academic Freedom in Europe: Time for a *Magna Charta*?', *Higher Education Policy* 2009, Vol. 22, No.2, pp. 163-189. Accepted manuscript available at: <http://eprints.lincoln.ac.uk/id/eprint/1611/1/ProofHEPArticle2For_Repository.pdf>.

Karran and Beiter 2020

T. Karran and K.D. Beiter, 'Academic freedom in the European Union: legalities and realities', in: S. Bergan, T. Gallagher and I. Harkavy, *Academic Freedom, Institutional Autonomy and the Future of Democracy*, Council of Europe Higher Education Series No. 24, Strasbourg: Council of Europe Publishing 2020, pp. 121-138.

KNAW 2021

Koninklijke Akademie van Wetenschappen (KNAW, Royal Netherlands Academy of Arts and Science), *Academische vrijheid in Nederland: Een begripsanalyse en richtsnoer*, Amsterdam: KNAW 2021. Available at: <<https://www.know.nl/publicaties/academische-vrijheid-nederland>>.

Maassen et al (STOA, European Parliament) 2023

P. Maassen et al, *State of play of academic freedom in the EU Member States: Overview of de factor trends and developments*, Brussels: European Parliamentary Research Service (EPRS) 2023. Available at: <[https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU\(2023\)740231](https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2023)740231)>.

Maex and Bakker 2022

K. Maex and M. Bakker, 'The university in the age of platforms and algorithms', in: A.M. Cauce, Y. Flückiger and B. Van der Zwaan (Eds), *Universities as the fifth power? Opportunities, Risks and Strategies*, Geneva: Association Glion Colloquium 2022, pp. 39-50.

Matei 2020

L. Matei, 'Academic freedom, university autonomy and democracy's future in Europe', in: S. Bergan, T. Gallagher and I. Harkavy, *Academic Freedom, Institutional Autonomy and the Future of Democracy*, Council of Europe Higher Education Series No. 24, Strasbourg: Council of Europe Publishing 2020, pp. 29-40.

McGonagle 2021

T. McGonagle, Case note to ECtHR 4 May 2021, Appl. Nos. 41139/15 and 41146/15 (*Akdeniz and Others v. Turkey*), 30 August 2021, <https://www.ehrc-updates.nl/commentaar/211626?skip_boomportal_auth=1>.

Merton 1942

R.K. Merton, 'A Note on Science and Democracy', *Journal of Legal and Political Sociology* 1942, Vol. 1, pp. 115-126. Available via <<https://home.heinonline.org/>>

Metzger 1987-1988

W.P. Metzger, 'Profession and Constitution: Two Definitions of Academic Freedom in America', *Texas Law Review* 1987-1988, Vol. 66, pp. 1265-1322. Available via <<https://home.heinonline.org/>>.

Metzger 1955

W.P. Metzger, 'The German Contribution to the American Theory of Academic Freedom', *Bulletin of the American Association of University Professors (1915-1955)* 1955, Vol. 41, No. 2, pp. 214-230. Available via <<https://www.jstor.org/>>.

Padilla 2017

M. Padilla, *Technological Sovereignty Vol. 2*, Barcelona: Descontrol 2017. Available at: <<https://www.ritimo.org/IMG/pdf/sobtech2-en-with-covers-web-150dpi-2018-01-10.pdf>>.

Roberts et al 2021

H. Roberts et al, 'Safeguarding European values with digital sovereignty: an analysis of statements and policies', *Internet Policy Review* 2021, Vol. 10, No. 3.

Sarooshi 2004

D. Sarooshi, 'Sovereignty, Economic Autonomy, the United States, and the International Trading System: Representations of a Relationship', *EJIL* 2004, Vol. 15, No. 4, p. 651-676.

Scholars at Risk 2020

Scholars at Risk, *Report to the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: Protection of Academic Freedom under International Human Rights Law*, New York: Scholars at Risk 2020. Available under 'inputs' at: <<https://www.ohchr.org/en/calls-for-input/report-academic-freedom-and-freedom-opinion-and-expression>>.

Scholars at Risk 2019

Scholars at Risk, *Promoting Higher Education Values: A Guide for Discussion*, New York: Scholars at Risk 2019. Available at: <<https://www.scholarsatrisk.org/resources/promoting-higher-education-values-a-guide-for-discussion/>>.

Smith 2020

T. Smith, 'Understanding the nature and scope of the right to science through the *Travaux Préparatoires* of the Universal Declaration of Human Rights and the International Covenant on Economic, Social and Cultural Rights', *The International Journal of Human Rights* 2020, Vol. 24, No. 8, pp. 1156-1179.

Steele and Rickards 2021

W. Steele and L. Rickards, 'The Role of the University in Society', in: *The Sustainable Development Goals in Higher Education: A Transformative Agenda?*, Cham: Springer Nature 2021, pp. 67-106.

Taştan and Ördek 2020

O. Taştan and A. Ördek, *A Report on Academic Freedoms in Turkey in the Period of the State Emergency*, Ankara: KAGED 2020. Available at:

<https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Submissions/Academics/INSAN_HAK_LARI_OKULU3.pdf>.

Timbermont 2022

E. Timbermont, 'Academic Freedom as a Fundamental Feature of Academia: A European Union Perspective', *Higher Education Policy* 2022.

Vaidhyanathan 2011

S. Vaidhyanathan, *The Googlization of Everything (and why we should worry)*, Berkeley: University of California Press 2011.

Vrieling et al 2023

J. Vrieling et al, *Challenges to academic freedom as a fundamental right*, Leuven: LERU 2023. Available at <<https://www.leru.org/publications/challenges-to-academic-freedom-as-a-fundamental-right>>.

Wolff 2000

K. Wolff, 'Academic freedom and university autonomy', in: Neave, G., *The universities' responsibilities to society: international perspectives*, Oxford: Elsevier Science 2000, pp. 196-205.

Ziegler 2019

T.D. Ziegler, 'Academic Freedom in the European Union – Why the Single European Market is a Bad Reference Point' (Research Paper), *Max Planck Institute for Comparative Public Law & International Law (MPIL)*, 2019. Available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3317406>.

Declarations and statements

The Guild 17 May 2022

The Guild, *Diversity, sustainability and quality must be the hallmarks of academic publishing in Europe*, 17 May 2022, <<https://www.the-guild.eu/news/2022/diversity-sustainability-and-quality-must-be-the-h.html>>.

Joint Statement by ALLEA, EUA and Science Europe 2019

Joint Statement by ALLEA, EUA and Science Europe, *Academic freedom and institutional autonomy: Commitments must be followed by action*, 10 April 2019, <<https://allea.org/allea-eua-and-science-europe-publish-joint-statement-on-academic-freedom-and-institutional-autonomy/>>.

Science Europe 2022

Science Europe, *Position statement: A values framework for the organisation of research 2022*, Brussels: Science Europe AISBL 2022. Available at: <<https://www.scienceeurope.org/our-resources/research-culture-values-framework/>>.

Blogposts, webpages, videos, other

International Association of Universities (IAU) Constitution 2019

International Association of Universities (IAU), *Constitution of the International Association of Universities*, amended in 2019. Available at: <<https://www.aaup.org/about/organization/aaup-constitution>>.

LERU New Year's Debate 2022

LERU, *LERU New Year's Debate 2022: The impact of EU data policy on university autonomy*, 28 January 2022. Video available at <<https://www.leru.org/news/new-years-debate>>.

KNAW Expertmeeting IV 2022

Koninklijke Akademie van Wetenschappen (KNAW, Royal Netherlands Academy of Arts and Science), *Expertmeeting IV: Wetenschap en digitale technologie*, 18 January 2022. Video available at: <<https://www.youtube.com/watch?v=CXIA3lucH28>>.

Newton 2013

C. Newton, 'Documentary throws the book at Google scanning project', 25 January 2013, CNET, <<https://www.cnet.com/tech/services-and-software/documentary-throws-the-book-at-google-scanning-project/>>.

Prosser 2015

D. Prosser, 'The costs of double dipping', 6 February 2015, Research Libraries UK, <<https://www.rluk.ac.uk/the-costs-of-double-dipping/>>.

STOA Academic Freedom Roundtable 2023

European Parliament, Panel for the Future of Science and Technology (STOA), *STOA Academic Freedom Roundtable: Freedom of scientific research and its legal protection in Europe* (workshop), 27 April 2023, <<https://www.europarl.europa.eu/thinktank/en/events/details/freedom-of-scientific-research-and-its-1/20230330WKS05181>>.

SURF and Kennisnet 2021 ('Value Compass')

SURF and Kennisnet, *Value Compass for digital transformation of education*, 2021. Value Compass available at: <<https://www.surf.nl/en/surf-magazine/launch-of-the-values-compass-in-2021>>.

Chapter 3

Case law

The Netherlands

CBb 12 July 2022, ECLI:NL:CBB:2022:411

Rb Rotterdam 4 March 2021, ECLI:NL:RBROT:2021:1766

Literature

ACCSS Open Letter 2021

ACCSS-initiative of Dutch cybersecurity professors, *Open Brief: overstappen naar de Cloud, bezint eer ge begint* (Open Letter), <<https://www.surf.nl/nieuws/reactie-van-de-universitaire-cios-op-de-open-brief-overstappen-naar-de-cloud-bezint-eer-ge>> and <<https://accss.nl/podium/open-brieven/overstappen-naar-de-cloud-bezint-eer-ge-begint/>>.

ACM Market Study Cloud Services 2022

Autoriteit Consument en Markt (ACM, Netherlands Authority for Consumers and Markets), *Market Study Cloud Services*, 5 September 2022, ACM/INT/440323, 2022. Available at: <<https://www.acm.nl/en/publications/market-study-cloud-services>>.

ACM Besluit 2019

ACM, 'Besluit tot verlening vergunning onder voorschriften voor concentratie Sanoma Learning B.V. en Iddink Holding B.V.', 28 augustus 2019, ACM/UIT/518704. For the English press release about the clearance, see <<https://www.acm.nl/en/publications/acm-conditionally-clears-acquisition-iddink-group-sanoma-learning>>.

Aouragh et al 2015

M. Aouragh et al, 'Let's First Get Things Done! On Division of Labour and Techno-political Practices of Delegation in Times of Crisis', *The Fibreculture Journal* 2015, Vol. 196, pp. 208-235.

Aspesi and Brand 2020

C. Aspesi and A. Brand, 'In pursuit of open science, open access is not enough', *Science* 2020, Vol. 368, No. 6491, pp. 575-577.

Aspesi et al 2019a (SPARC Landscape Analysis)

C. Aspesi et al, *Landscape Analysis: The Changing Academic Publishing Industry – Implications for Academic Institutions*, SPARC 2019. Available at: <<https://infrastructure.sparcopen.org/landscape-analysis>>.

Aspesi et al (SPARC) 2019b

C. Aspesi, et al, *A Roadmap for Action: Academic Community Control of Data Infrastructure*, Lincoln, Nebraska, USA: University of Nebraska 2019. Available at: <<https://digitalcommons.unl.edu/scholcom/130/>>.

Ausloos and Veale 2020

J. Ausloos and M. Veale, 'Researching with Data Rights', *Technology and Regulation* 2020, pp. 136-157.

Ausloos, Leerssen and Ten Thije 2020

J. Ausloos, P. Leerssen and T. ten Thije, 'Operationalizing Research Access in Platform Governance: What to Learn from Other Industries?', *Algorithm Watch* 2020. Available at: <<https://dare.uva.nl/search?identifier=90e4fa77-d59a-49f1-8ccd-57d0725122bd>>.

Autio et al 2018

E. Autio et al, 'Digital affordances, spatial affordances, and the genesis of entrepreneurial ecosystems', *Strategic Entrepreneurship Journal* 2018, Vol. 12, pp. 72-95.

Bok et al 2021 (VSNU)

C. Bok et al 2021, *Advies publieke waarden voor het onderwijs* (Werkgroep publieke waarden), Den Haag: VSNU 2021. Available at: <<https://www.universiteitenvannederland.nl/2020/publieke-waarden-en-academische-soeveriniteit.html>>.

Bosma and Huis in 't Veld 2022

B. Bosma and I. Huis in 't Veld, 'Onderwijsdigitalisering vereist bescherming van publieke waarden', in: Van Duuren, N., Nienhuis, J. and De Pous, V. (Eds.), *Multidisciplinaire aspecten van digital security*, Delex 2022.

DFG Briefing Paper 2021

Committee on Scientific Library Services and Information Systems of the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation), *Data tracking in research: aggregation and use or sale of usage data by academic publishers* (Briefing paper), 28 October 2021. Available at: <https://www.dfg.de/download/pdf/foerderung/programme/lis/datentracking_papier_en.pdf>.

Goldenfein et al 2019

J. Goldenfein et al, 'Private Companies and Scholarly Infrastructure – Google Scholar and Academic Autonomy, Digital Live Initiative', 21 October 2019, Cornell Tech, <<https://www.dli.tech.cornell.edu/post/private-companies-and-scholarly-infrastructure-google-scholar-and-academic-autonomy>>.

Institute for Information Law 2023b

Institute for Information Law, 'Information Law and the Digital Transformation of the University: Digital Sovereignty, Data Governance and Researchers' Access to Data – Part II. Access to Data for Research', 2023 <<https://www.ivir.nl/part-ii-access-to-data-for-research/>>.

Kemman and Te Velde 2021

M. Kemman and R. te Velde, *Feasibility study Open Knowledge Base*, Utrecht: VSNU 2021. Available at: <<https://www.dialogic.nl/en/2021/03/25/feasibility-of-an-open-knowledge-base/>>.

Kitchin 2014

R. Kitchin, *The Data Revolution. Big Data, Open Data, Data Infrastructures and Their Consequences*. London: Sage, 2014.

Maex and Bakker 2022

K. Maex and M. Bakker, 'The university in the age of platforms and algorithms', in: A.M. Cauce, Y. Flückiger and B. Van der Zwaan (Eds), *Universities as the fifth power? Opportunities, Risks and Strategies*, Geneva: Association Glion Colloquium 2022, pp. 39-50.

Maex 2021

K. Maex, 'Protect independent and public knowledge', *Lecture at the Dies Natalis of the University of Amsterdam*, 10 January 2021. Available at: <https://uva.uas.figshare.com/articles/presentation/Digital_University_Act_pdf/13553825>.

Maex et al 2019

K. Maex et al, 'Digitalisering bedreigt onze universiteit. Het is tijd om een grens te trekken', *de Volkskrant* 22 December 2019.

Rieder and Hofmann 2020

B. Rieder and J. Hofmann, 'Towards platform observability', *Internet Policy Review* 2020, Vol. 9, No. 4.

Roosendaal 2023

A. Roosendaal, 'The GDPR as a means to protect digital sovereignty of universities' (Expert Memo), 2023 <<https://www.ivir.nl/expert-memo>>.

Ruggieri 2022

F. Ruggieri, 'National cloud strategies, digital sovereignty, and community: a vision', *Connect – The Magazine from the GÉANT Community*, June 2022. Available at: <<https://connect.geant.org/wp-content/uploads/2022/06/GEANT-CONNECT-40-CONNECT-Magazine.pdf>>.

Schaafsma and Van der Meer 2022

J. Schaafsma and M. van der Meer, 'Universiteiten zitten te slapen, grote uitgevers gaan er met hun data vandoor', *NRC* 8 May 2022.

Schumann and Simantke 2017 (Investigate Europe)

H. Schumann and E. Simantke (Investigate Europe), 'Cyber-Attacken auf staatliche IT Europas fatale Abhängigkeit von Microsoft', *Tagesspiegel* 13 May 2017, <<https://www.tagesspiegel.de/gesellschaft/europas-fatale-abhaengigkeit-von-microsoft-3821812.html>>.

Seifried et al 2021

M. Seifried et al, *Schwerpunktstudie Digitale Souveränität – Bestandaufnahme und Handlungsfelder*, Berlin: Bundesministerium für Wirtschaft und Energie (BMWi) 2021. Available at: <<https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/schwerpunktstudie-digitale-souveranitaet.html>>.

Sellar and Hogan 2019

S. Sellar and A. Hogan, *Pearson 2025: Transforming teaching and privatizing education data*, Brussels: Education International 2019. Available at: <<https://www.ei-ie.org/en/item/25681:pearson-2025-transforming-teaching-and-privatising-education-data>>.

SPARC 2022 (Interfolio Acquisition Report)

SPARC, 'Possible Negative Impacts from Elsevier's Increased Market Power', in: SPARC, *Elsevier's Acquisition of Interfolio: Risks and Responses*, 29 June 2022. Available at: <<https://infrastructure.sparcopen.org/interfolio-acquisition>>.

SPARC 2020 (Dutch Consortia/Elsevier Contract)

SPARC, *The Dutch Consortia/Elsevier Contract: The Real Risks*, 28 May 2020. Available at: <<https://infrastructure.sparcopen.org/dutch-consortia-elsevier-contract>>.

Tanczer et al 2016

L. Tancze et al, 'Censorship and Surveillance in the Digital Age: The Technological Challenges for Academics', *Journal of Global Security Studies* 2016, Vol. 1, No. 4, pp. 346-355.

University of California, UCACC and UCOLASC 2019

University of California, University Committee on Academic Computing and Communications (UCACC) and University Committee on Library and Scholarly Communication (UCOLASC), *Concerns Regarding the Use of Research Information Management Systems (RIMS)*, 12 March 2019. Available at: <<https://senate.universityofcalifornia.edu/files/reports/rm-jn-mb-rims.pdf>>.

Van Daalen 2022

O. van Daalen, *Making and breaking with science and conscience: the human rights-compatibility of information security governance in the context of quantum computing and encryption* (dissertation, Amsterdam UvA), Amsterdam 2022.

Williamson 2021

B. Williamson, 'Making markets through digital platforms: Pearson, edu-business, and the (e)valuation of higher education', *Critical Studies in Education* 2021, Vol. 62, No. 1, pp. 50-66.

Williamson and Hogan 2021

B. Williamson and A. Hogan, *Pandemic Privatisation in Higher Education: Edtech & University Reform*, Brussels: Education International 2021. Available at: <<https://www.ei-ie.org/en/item/25245:pandemic-privatisation-in-higher-education-edtech-university-reform>>.

Williamson and Hogan 2020

B. Williamson and A. Hogan, *Commercialisation and privatisation in/ of education in the context of Covid-19*, Brussels: Education International 2020. Available via: <<https://eprints.qut.edu.au/216577/>>.

Williamson 2016

B. Williamson, 'Digital education governance: data visualization, predictive analytics, and 'real-time' policy instruments', *Journal of Education Policy* 2016, Vol. 31, No. 2, pp. 121-141.

Wilkinson et al 2016

M.D. Wilkinson, M. Dumontier, Ij. J. Aalbersberg, et al. 'The FAIR Guiding Principles for scientific data management and stewardship', *Scientific Data* 2016, Vol. 3, No. 1. Available via <https://www.doi.org/10.1038/SDATA.2016.18>.

Declarations and statements

ALLEA Statement on Open Access, 12 December 2022

ALLEA and B. Hugenholtz, *Statement on Open Access Publication under "Big Deals" and the New Copyright Rules*, 12 December 2022. Available at: <http://copyrightblog.kluweriplaw.com/2022/12/12/allea-statement-on-open-access-publication-under-big-deals-and-the-new-copyright-rules/>.

Blogposts, webpages, videos, other

Baio 2022

A. Baio, 'AI Data Laundering: How Academic and Nonprofit Researchers Shield Tech Companies from Accountability', 30 September 2022, WAXY, <https://waxy.org/2022/09/ai-data-laundering-how-academic-and-nonprofit-researchers-shield-tech-companies-from-accountability/>.

CBS News 2022

CBS News, 'LexisNexis illegally collected and sold people's personal data, lawsuit alleges', 16 August 2022, <https://www.cbsnews.com/news/lexisnexis-lawsuit-collected-sold-personal-data-immigration-advocates-allege/>.

De Rijcke 2020

S. de Rijcke, 'Elsevier and the Dutch Open Science goals', 20 May 2020, Leiden Madtrics, <https://www.leidenmadtrics.nl/articles/s-de-rijcke-cwts-leidenuniv-nl>.

Hoepman 2021

J.H. Hoepman, 'Universities need to Act, Digitally (We don't need a Digital University Act)', 10 January 2021, <https://blog.xot.nl/2021/01/10/universities-need-to-act-digitally-we-don-t-need-a-digital-university-act/index.html>.

Gürses 2020

S. Gürses, 'What happened when the university went online?' (Part 1-4) (video), ArtEZ University of Arts, <https://www.youtube.com/watch?v=pXFslDTSyk&list=PLDp0FMQdH3yIEGRhnsjKfC784OF74dYr&index=6>.

De Knecht 2019

S. de Knecht, 'Leaked document on Elsevier negotiations sparks controversy', 6 November 2019, ScienceGuide, <https://www.scienceguide.nl/2019/11/leaked-document-on-elsevier-negotiations-sparks-controversy/>.

Leland 2021

J. Leland, 'What Zoom Does to Campus Conflicts over Israel and Free Speech', *The New York Times* 22 January 2021.

Mastrolonardo 2016

R. Mastrodonato, 'From Microsoft to LibreOffice: How Italy's military is starting its march to open source', 30 June 2016, ZDNET, <<https://www.zdnet.com/article/from-microsoft-to-libreoffice-how-italys-military-is-starting-its-march-to-open-source/>>.

Másson Maack 2017

M. Másson Maack, 'Europe is living under Microsoft's digital killswitch', 10 May 2017, TNW, <<https://thenextweb.com/news/europe-is-living-under-microsofts-digital-killswitch>>.

NOS 2019

NOS, 'Universiteit Maastricht kampt met ransomware-aanval', 24 December 2019, <<https://nos.nl/artikel/2316120-universiteit-maastricht-kampt-met-ransomware-aanval>>.

NYU AAUP Statement 23 October 2020

American Association of University Professors (AAUP) New York University, 'Statement on Zoom Censorship', 23 October 2020, <<https://www.nyu-aaup.org/statement-on-zoom-censorship/>>.

Open Science Platform Products and Services Agreement of 15 May 2020

SURF and Elsevier B.V., *Open Science Platform Products and Services Agreement*, signed on 15 May 2020. Available via: <https://www.universiteitenvannederland.nl/en_GB/open-science-agreement-with-elsevier.html>.

Sabel 2020

P. Sabel, 'Google-storing komt hard aan', *de Volkskrant* 15 December 2020.

Schaafsma and Van der Meer 2021

J. Schaafsma and M. Van der Meer, 'Pure' misery: how Open Access makes us more dependent on big publishers', 15 November 2021, *Univers – the independent news source of Tilburg University*, <<https://universonline.nl/nieuws/2021/11/15/pure-misery-how-open-access-makes-us-more-dependent-on-big-publishers/>>.

Schaer 2020

C. Schaer, 'Linux not Windows: Why Munich is shifting back from Microsoft to open source – again', 14 May 2020, ZDNET, <<https://www.zdnet.com/article/linux-not-windows-why-munich-is-shifting-back-from-microsoft-to-open-source-again/>>.

Schonfeld 2018

R.C. Schonfeld, 'Workflow Lock-in: A Taxonomy', 2 January 2018, *The scholarly kitchen*, <<https://scholarlykitchen.sspnet.org/2018/01/02/workflow-lock-taxonomy/>>.

VSNU Dutch Taskforce on Responsible Management of Research Information and Data

VSNU (Association of Dutch Universities, now known as UNL), *Dutch Taskforce on Responsible Management of Research Information and Data* (Founding Document). Available at: <<https://www.universiteitenvannederland.nl/files/documenten/Domeinen/Onderzoek/Open%20access/Engelstalige%20samenvatting%20opdracht%20werkgroep.pdf>>.

VSNU Guiding Principles developed by the Dutch Taskforce on Responsible Management of Research Information and Data 2020 (first version)

VSNU (Association of Dutch Universities, now known as UNL), *Guiding Principles on Management of Research Information and Data*, 11 May 2020, <https://universiteitenvannederland.nl/files/documenten/Nieuwsberichten/Guiding%20Principles%20on%20Management%20of%20Research%20Information%20and%20Data_11May.pdf>.

VSNU Guiding Principles developed and revised by the Dutch Taskforce on Responsible Management of Research Information and Data 2020 (second version)

VSNU (Association of Dutch Universities, now known as UNL), *Seven Guiding Principles For Open Research Information*, 14 February 2022, <<https://zenodo.org/record/6074944#.Y8hLchXMI2x>>.

Quintais 2023

J.P. Quintais, 'Generative AI, Copyright and the AI Act', 9 May 2023, *Kluwer Copyright Blog*. Available at: <<https://copyrightblog.kluweriplaw.com/2023/05/09/generative-ai-copyright-and-the-ai-act/>>.

Chapter 4

Legislation

European Union

Primary EU Law

Treaty on the Functioning of the European Union (TFEU), consolidated version, OJ EU C 326/47.

Directives and regulations

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, amended by Directive 2013/37/EU [no longer in force].

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

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

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast).

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).

Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June on promoting fairness and transparency for business users of online intermediation services.

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 November 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

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).

Legislative proposals

Proposal for a Directive on the re-use of public sector information (recast), COM(2018) 234 final, 24 April 2018 [adopted as Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information].

Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM/2021/206 final.

- Latest version: European Parliament, Committee on the Internal Market and Consumer Protection and Committee on Civil Liberties, Justice and Home Affairs, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 16 May 2023, COM(2021)0206 – C9 0146/2021 – 2021/0106(COD)).

Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM/2022/68 final.

- Latest version: Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) – Mandate for negotiations with the European Parliament, 17 March 2023, 7413/23.

Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM(2022) 197 final.

The Netherlands

Existing laws

Wet hergebruik van overheidsinformatie, <<https://wetten.overheid.nl/BWBR0036795/2021-07-01>>.

Legislative proposals

Wijziging van de Wet hergebruik overheidsinformatie en enkele andere wetten in verband met de implementatie van richtlijn br. 2019/1024/EU van het Europees Parlement en de Raad van 20 juni 2019 inzake open data en het hergebruik van overheidsinformatie (Wet implementatie Open data richtlijn), <<https://zoek.officielebekendmakingen.nl/dossier/kst-36382-2.html#extrainformatie>>.

Policy documents

European Union

European Commission, Communication on a European Cloud Initiative – Building a competitive data and knowledge economy in Europe, 19 April 2016, COM(2016) 178 final.

European Commission, Communication on Artificial Intelligence for Europe, 25 April 2018, COM(2018) 237 final.

European Commission, Recommendation (EU) 2018/790 of 25 April 2018 on access to and preservation of scientific information.

Independent High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, 8 April 2019. Available at: <<https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html>>.

European Commission, White Paper on Artificial Intelligence – A European approach to excellence and trust, 19 February 2020, COM(2020) 65 final.

European Commission, Communication on a European strategy for data, 19 February 2020, COM(2020) 66 final.

European Commission, Communication on Shaping Europe’s digital future, 19 February 2020, COM(2020) 67 final.

European Commission, Communication on a New Era for Research and Innovation, 30 September 2020, COM(2020) 628 final.

Council conclusions on the New European Research Area, 1 December 2020, 13567/20. Available at: <<https://www.consilium.europa.eu/en/documents-publications/public-register/public-register-search/results/?AllLanguagesSearch=False&OnlyPublicDocuments=False&DocumentNumber=13567%2F20&DocumentLanguage=en>>.

European Commission, Communication on the 2030 Digital Compass: the European way for the Digital Decade, 9 March 2021, COM(2021) 118 final.

Council Recommendation (EU) 2021/2122 of 26 November 2021 on a Pact for Research and Innovation in Europe, OJ EU L 431/1.

European Commission, ‘European Research Policy Agenda – Overview of actions for the period 2022-2024’, November 2021.

European Commission, Communication establishing a European Declaration on Digital rights and principles for the Digital Decade, 26 January 2022, COM(2022) 27 final.

European Commission, *European Declaration on Digital Rights and Principles for the Digital Decade*. Signed version available via: <<https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles>>.

European Commission, Commission Staff Working Document: Better Regulation Guidelines, SWD(2021) 305 final.

European Commission, ‘Better Regulation Toolbox’, July 2023. Available at: <https://commission.europa.eu/law/law-making-process/planning-and-proposing-law/better-regulation/better-regulation-guidelines-and-toolbox_en>.

The Netherlands

Dutch legislative proposal implementing the Open Data Directive (*Wet implementatie Open data richtlijn*). Available at: <<https://wetgeving.skalender.overheid.nl/regeling/WGK009986/documenten/Raad%20van%20State/Adviesaanvrage%20aanhangig%20bij%20Raad%20van%20State/1>>.

Advisory Division of the Dutch Council of State, Advice on Dutch legislative proposal implementing the Open Data Directive (*Advies van de Afdeling advisering van de Raad van State inzake het wetsvoorstel tot implementatie van de Open data richtlijn*). Available at: <<https://www.raadvanstate.nl/actueel/nieuws/oktober/samenvatting-open-data-richtlijn/@132262/w04-22-0141/>>.

Other

Explanatory Memorandum to the German proposal implementing the Open Data Directive (*Entwurf eines Gesetzes zur Änderung des E-Government-Gesetzes und zur Einführung des Gesetzes für die Nutzung von Daten des öffentlichen Sektors*), pp. 22-23. Available at: <<https://dsrserver.bundestag.de/btd/19/274/1927442.pdf>>.

Case law

CJEU 16 September 2016, C-484/14 (*Mc Fadden v. Sony Music*).

CJEU 12 July 2012, C-138/11 (*Compass-Datenbank v. Austria*).

Literature

Araujo et al 2022

T. Araujo et al, 'OSD2F: An Open-Source Data Donation Framework', *Computational Communication Research*, Vol. 4, No. 2, pp. 372-387.

European Commission and PPMI et al 2024 (forthcoming)

European Commission and PPMI et al, *Study to evaluate the effects of the EU copyright framework on research and the effects of potential interventions and to identify and present relevant provisions for research in EU data and digital legislation, with a focus on rights and obligations* – RTD/2023/SC/01, forthcoming 2024.

European Commission and Angelopoulos 2022

European Commission, Directorate-General for Research and Innovation, C. Angelopoulos, *Study on EU copyright and related rights and access to and reuse of scientific publications, including open access: exceptions and limitations, rights retention strategies and the secondary publication right*, Brussels: Publications Office of the European Union 2022, <<https://data.europa.eu/doi/10.2777/891665>>.

European Commission and Lundqvist 2022

European Commission, Directorate-General for Research and Innovation, B. Lundqvist, *Study on the Digital Services Act and Digital Markets Act and their possible impact on research*, Brussels: Publications Office of the European Union 2022, <<https://data.europa.eu/doi/10.2777/751853>>.

European Commission and Senftleben 2022

European Commission, Directorate-General for Research and Innovation, M. Senftleben, *Study on EU copyright and related rights and access to and reuse of data*, Brussels: Publications Office of the European Union 2022, <<https://data.europa.eu/doi/10.2777/78973>>.

European Commission and Van Eechoud 2022

European Commission, Directorate-General for Research and Innovation, M. Van Eechoud, *Study on the Open Data Directive, Data Governance Act and Data Act and their possible impact on research*, Brussels: Publications Office of the European Union 2022, <<https://data.europa.eu/doi/10.2777/71619>>.

European Commission, Mendez and Lawrence 2020

European Commission, Directorate-General for Research and Innovation, Mendez, E., Lawrence, R., *Progress on open science: towards a shared research knowledge system: final report of the open science policy platform*, Brussels: Publications Office 2020, <<https://op.europa.eu/en/publication-detail/-/publication/d36f8071-99bd-11ea-aac4-01aa75ed71a1>>.

European Commission Communication 2017

Communication from the European Commission, 'Building a European Data Economy', 10 January 2017, COM(2017) 9 final.

Gulati-Gilbert and Seamans 2023

S. Gulati-Gilbert and R. Seamans, 'Data portability and interoperability: A primer on two policy tools for regulation of digitized industries', Brookings Institution, United States of America (2023), <<https://www.brookings.edu/articles/data-portability-and-interoperability-a-primer-on-two-policy-tools-for-regulation-of-digitized-industries/>>.

Institute for Information Law 2023b

Institute for Information Law, 'Information Law and the Digital Transformation of the University: Digital Sovereignty, Data Governance and Researchers' Access to Data – Part II. Access to Data for Research', 2023 <<https://www.ivir.nl/part-ii-access-to-data-for-research/>>.

Kitchin 2014

R. Kitchin, *The Data Revolution. Big Data, Open Data, Data Infrastructures and Their Consequences*. London: Sage, 2014.

Lundqvist 2013

B. Lundqvist, 'Turning Government Data Into Gold': The Interface Between EU Competition Law and the Public Sector Information Directive With Some Comments on the Compass Case', *International Review of Intellectual Property and Competition Law* 2013, Vol. 44, pp. 79-95.

Mons 2020

B. Mons, 'Invest 5% of research funds in ensuring data are reusable', *Nature* 2020, Vol. 578, p. 491. Available at: <<https://www.nature.com/articles/d41586-020-00505-7>>.

Rajam 2020

N. Rajam, 'The impact of trade secrets for publicly funded research collaborations in Europe', in: J. Schovbo, T. Minssen and T. Riis (Eds.), *The Harmonization and Protection of Trade Secrets in the EU*, Cheltenham: Edward Elgar 2020, pp. 295-319.

Van Dijck, Poell and De Waal 2018

J. Van Dijck, T. Poell and M. de Waal, *The Platform Society: Public Values in a Connective World*, Oxford: Oxford University Press 2018.

Van Eechoud 2023

M. van Eechoud, 'FAIR, FRAND and open – the institutionalization of research data sharing under the EU data strategy', in: S. Frankel et al (Eds.), *Improving Intellectual Property. A Global Project*, Cheltenham: Edward Elgar 2023, pp. 320-330.

Van Wijnen and Olsthoorn 2021

F. Van Wijnen and S. Olsthoorn, 'Waarom KLM zelfs data uit de airco verzamelt', *Het Financieele Dagblad* 30 September 2021.

Zuiderwijk, Shinde and Jeng 2020

A. Zuiderwijk, R. Shinde and W. Jeng, 'What drives and inhibits researchers to share and use open research data? A systematic literature review to analyze factors influencing open research data adoption', *PLoS ONE* 2020, Vol. 15, No. 9.

Declarations and statements

ALLEA Statement on IPRs and Open Science

ALLEA Statement, *Aligning intellectual property rights with open science*, April 2022. Available at: <<https://rac.es/ficheros/doc/4147faecdc331ea0.pdf>>.

Joint statement of CESAER, COAR and LIBER 2022

Joint Statement by CESAER, COAR and LIBER, *Scientific knowledge must be protected to ensure a Europe fit for the digital age*, 24 January 2022. Available at: <<https://www.cesaer.org/content/5-operations/2022/20220124-joint-statement-scientific-knowledge-must-be-protected-to-ensure-a-europe-fit-for-the-digital-age.pdf>>.

Joint statement by Research Organisations, Libraries, Repositories and University Networks 2022

Statement by Research Organisations, Libraries, Repositories and University Networks, *On the exemption of not-for-profit educational and scientific repositories, digital archives and libraries from the Digital Services Act*, 5 April 2022. Available at: <<https://www.scienceurope.org/our-resources/dsa-statement/>>.

Blogposts, webpages, videos and other

Academic Freedom Roundtable 2023

Panel for the Future of Science and Technology (STOA), ‘Academic Freedom Roundtable: Freedom of scientific research and its legal protection in Europe’, European Parliament, 27 April 2023. Webstream available at: <<https://www.europarl.europa.eu/thinktank/en/events/details/freedom-of-scientific-research-and-its-1/20230330WKS05181>>.

Corona Data Donation App

Corona-Datenspende (app), <<https://corona-datenspende.de/science/en/>>.

“Data for Good”-initiative

Data for Good Foundation (platform), <<https://dataforgoodfoundation.com/en/>>.

Deketelaere 2021

K. Deketelaere, ‘The EU must write its research ambitions into law’, 13 May 2021, ResearchProfessional News, <<https://www.researchprofessionalnews.com/rr-news-europe-views-of-europe-2021-5-the-eu-must-write-its-research-ambitions-into-law/>>.

Ehler 2023

C. Ehler, ‘Intellectual superiority will not protect academic freedom’, 11 May 2023, ResearchProfessional News, <<https://www.researchprofessionalnews.com/rr-news-europe-views-of-europe-2023-5-intellectual-superiority-will-not-protect-academic-freedom/>>.

EOSC Projects

EOSC Projects (webpage), <<https://eosc-portal.eu/about/eosc-projects>>.

European Commission Digital Services Act package webpage

European Commission, Policies > The Digital Services Act package (webpage), <<https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>>.

European Commission Open Science webpage

European Commission, Strategy on research and innovation > Strategy 2020-2024 > Our digital future > Open Science (webpage), <https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/our-digital-future/open-science_en>.

European Parliament Digital Agenda Factsheet

European Parliament, ‘Digital Agenda For Europe’ (webpage/factsheet), <<https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe>>.

SWIPO Codes of Conduct

SWIPO Codes of Conduct, <<https://swipo.eu/download-section/copyrighted-downloads/>>.

Prior information notice d.d. 4 May 2022 in the EU's public procurement journal (TED)

Tenders Electronic Daily (TED), *Prior information notice for Managed Services for the European Open Science Cloud Platform*, 4 May 2022, CNECT/LUX/2022/CD/0023, <<https://ted.europa.eu/udl?uri=TED:NOTICE:234660-2022:TEXT:EN:HTML&src=0>>.