Digital Cloud Services and Higher Education: The Quest for Data Autonomy

Oskar J. Gstrein

* Ambassador Data Autonomy University of Groningen, Programme Director BSc Data Science and Society, Assist. Prof. Governance and Innovation at Faculty Campus Fryslân

Draft for Ars Aequi, 27 February 2023

Trailer

Universities are increasingly dependent on cloud-based data infrastructure and services. They migrate 'their local data' now for more than a decade, yet many fundamental questions remain. We need a profound discussion about this paradigmatic shift, which heavily affects the autonomy of students, staff, and higher education as such. There is a lack of exit-strategies, AI-based inferences might deprive students and institutions of fundamental choices, and the data generated with public money is volatile for extraction by powerful actors.

1. Introduction

A longitudinal study covering the period from January 2015 until June 2021 found that the use of cloud-based data storage services among Dutch universities offered either by Amazon, Google or Microsoft increased from approximately 50% to 100%.[1] The pre-print study includes numbers on the use of cloud-based e-mail services by Dutch and international universities, or use of services such as Google Workspace and Microsoft 365. It also documents an increasing dependence on learning management systems such as Blackboard and Brightspace, as well as conferencing services like Zoom.[2] Such cloud-based services gain more influence as local IT-centres on premises – e.g. providing storage for researchers or hosting university e-mail services – decrease in relevance. While the datafication of education is a broader trend that raises questions about the autonomy of students and pupils,[3] one of the most surprising findings from the empirical study is that the COVID-19 pandemic did not accelerate this process of datafication, since it was already in full swing.[4]

While 'cloud infrastructures' promise efficiency and convenience,[5] the power of public institutions to make fundamental decisions about 'their' data seems to disappear. With the transition of both data storage and applications to data centres, laptops and desktop computers increasingly become end-user terminals to access platforms (e.g. Google's 'Chromebook'). At the same time, a centralisation of information collection and processing

[1] T. Fiebig, S. Gürses, C. H. Gañán et al., 'Heads in the Clouds: Measuring the Implications of Universities Migrating to Public Clouds', Pre-print available at SocArxiv, https://arxiv.org/abs/2104.09462 (25 Jan 2023), p. 5.

[2] Fiebig et al. 2023, p. 5-8.

[3] T. Henne, O.J. Gstrein, 'Governing the 'Datafied' School: Bridging the Divergence between Universal Education and Student Autonomy', in: A. Zwitter, O.J. Gstrein (eds.), *Handbook on the Politics and Governance of Big Data and Artificial Intelligence*, Cheltenham – UK, forthcoming June 2023.

[4] Fiebig et al. 2021.

[5] According to ISO standard 17788 cloud computing can be defined as a 'paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.' More information is available at: https://www.iso.org/standard/60544.html (27 Jan 2023).

occurs.[6] These developments raise data protection concerns as identified by the Dutch and European data protection authorities,[7] challenge territorial and societal integrity,[8] and – potentially most importantly – undermine the autonomy of individuals and organisations to make meaningful decisions about the data they produce and share. This ability to make meaningful decisions about data will be referred to as 'data autonomy' and remains at the centre of this article.[9]

In France and Germany first actions are taken to ban the use of cloud-based services such as Microsoft 365 or Google Workspace in an educational context. In contrast, the cooperative association of the Dutch educational and research institutions (SURF) states that negotiations and agreements can resolve the concerns.[10] In a world that is rife with difficult challenges and daunting tasks, it is hard to remain focused and identify priorities. Against this background it is understandable that people and institutions are happy if things 'just work', without devoting too much attention or asking critical questions. However, when it comes to the slow and persistent change of the data infrastructure that we are dependent on in higher education, a transition might slowly take place that results in profound and irreversible

[6] B. J. Jütte, G. Noto La Diega, G. Priora, G. Salza, 'Zooming in on Education: An Empirical Study on Digital Platforms and Copyright in the United Kingdom, Italy, and the Netherlands', *European Journal of Law and Technology* 2022.

[7] Autoriteit Persoonsgegevens, Brief over inzet cloud service providers, https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_over_inzet_cloud_service_providers.pdf (25 Jan 2023). European Data Protection Board, Launch of coordinated enforcement on use of cloud by public sector, https://edpb.europa.eu/news/news/2022/launch-coordinated-enforcement-use-cloud-public-sector_nl (25 Jan 2023).

[8] A. Baur, 'European Dreams of the Cloud: Imagining Innovation and Political Control', *Geopolitics* 2023, DOI: 10.1080/14650045.2022.2151902, p. 1-3.

[9] For an overview on related concepts see O.J. Gstrein, A. Beaulieu, 'How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches', *Philosophy & Technology* 2022, afl. 35 – 3.

[10] Science Guide, SURF: 'Verbod gebruik Microsoft in Nederlands onderwijs niet nodig', https://www.scienceguide.nl/2022/12/surf-verbod-gebruik-microsoft-in-nederlands-onderwijs-niet-nodig/ (25 Jan 2023).

consequences.[11] These changes have the potential to undermine the individual and collective autonomy of the higher education sector, depriving us of the possibility to shape our future in the way that we believe it should be.

The case of publicly funded universities is particularly interesting. On the one hand, they are based on public values and governed by laws. 'Academic freedom',[12] free expression and independence of thought, as well as institutional independence are at their core. They are destined to become lighthouses of creative and critical thinking. Universities are involved in developing open-source applications for teaching and research. On the other hand, as public institutions universities are required to use funds efficiently, and provide state-of-the-art working and research environments for students, researchers, and staff.

In light of these contrasting requirements, what should higher education do to address the increasing dependence on 'Big Tech' pursuing commercial interests, while increasing data autonomy? This article first explores this question from a data protection perspective, before turning to the broader governance implications. Here the view on academic freedom in the context of a republican understanding of freedom plays an essential role. The text then further elaborates on the concept of data autonomy and highlights its relevance by considering two examples in detail. In conclusion, it will be argued that we cannot be pragmatic when it comes to data autonomy. We must demand to keep principles and values in focus.

---

[11] T. Ansari, A. Beaulieu, T.F. Blauth et al., 'De universiteit als duurste streamingdienst? De gevolgen van een veranderde infrastructuur', *THEMA Tijdschrift voor Hoger Onderwijs en Management* 2020, 5, p. 51-54.

[12] In the Charter of Fundamental Rights of the European Union academic freedom is enshrined in Article 13, together with the Freedom of the Arts. The explanatory note to Article 13 states that the right is primarily deduced from the right to freedom of thought and expression. According to UNESCO's Recommendation concerning the Status of Higher Education Teaching Personnel, academic freedom entails (1) institutional autonomy, (2) individual rights and freedoms to expression, (3) protection provided by the state. A 2020 report by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, cited the UNESCO Recommendation and stated further that academic freedom involves institutional protections, including autonomy and self-governance. For more information see S. Peers, T. Hervey, J. Kenner and A. Ward (eds.), *The EU Charter of Fundamental Rights: A Commentary*. *Article 13*. Oxford: Hart Publishing, 2021, p. 405–428.

2. This is (not) about data protection

The first aspects that come to mind when considering the dependency of higher education on cloud infrastructure are related to privacy and data protection. Indeed, the European Data Protection Board (EDPB) – a body constituted by the 2016 European Union General Data Protection Regulation (GDPR) that assembles all national data protection authorities of EU member states – presented on 17 January 2023 preliminary findings on the use of cloud-based services by the public sector.[13] This initiative entails an analysis of the use of cloud services by the entire public sector. While the report shares first insights, the entire initiative is not finished with this publication.

In its report the EDPB identifies eight challenges, which can be summarised under three main themes. The first theme relates to a lack of clarity relating to actual data flows. It manifests through missing data protection impact assessments (or risk assessments), the lack of knowledge about the involvement of sub-processors handling personal data, as well as international data transfers that give foreign authorities access to the data transferred – think of the Snowden revelations,[14] or the alleged access of the Chinese government to data collected by private companies such as ByteDance, which developed the app TikTok.[15]

The second theme relates to an unclarity of responsibilities and duties. It manifests in confusion about the formal role of the parties, as well as the lack of contracts. The third theme relates to a lack of control, which results in the inability of public authorities to negotiate tailored contracts with cloud service providers, as well as the processing and auditing of

[13] European Data Protection Board, Coordinated Enforcement Action - use of cloud-based services by the public sector, https://edpb.europa.eu/our-work-tools/our-documents/report/coordinated-enforcement-action-use-cloud-based-services-public_en (27 Jan 2023).

[14] E. Snowden, *Permanent Record*, New York City: Metropolitan Books, 2019.

[15] D. Bondy Valdovinos Kaye, X. Chen, J. Zeng, 'The co-evolution of two Chinese mobile short video apps: Parallel platformization of Douyin and TikTok', *Mobile Media & Communication* 2021, afl. 9 – 2, p. 229–253.

telemetry data by the providers.[16] This latter aspect is highly technical, yet critical. As users interact with apps such as those included in Microsoft 365, data is being collected by the provider to understand usage patterns and user behaviour (e.g. analysing clicking patterns, feature use, etc.). This data can be used to profile user groups or target them with ads, as well as improve the services. Collection of telemetry data is particularly sensitive when such apps are used by government ministries,[17] or educational institutions which cannot function effectively without them.

The EDPB report further mentions the interaction of supervisory authorities with universities. Both in Italy and Portugal the use of a proctoring software transferring sensitive biometric data of students to third countries outside the European Union was stopped after investigation.[18] The assumption in European data protection law is that such transfers are by default unsafe and illegal,[19] unless there is an adequacy decision by the European Commission, or specific private contracts are in place.[20]

While this initiative of the data protection authorities to clarify the situation in the public sector is welcome, the preliminary results are simply frustrating. The challenges identified

[16] European Data Protection Board, 2022 Coordinated Enforcement Action - use of cloud-based services by the public sector, https://edpb.europa.eu/our-work-tools/our-documents/report/coordinated-enforcement-action-use-cloud-based-services-public_en (27 Jan 2023), p. 2, 10-21.

[17] For a detailed report see Ministerie van Justitie en Veiligheid, DPIA Office 365 Online and mobile Office apps (June 2019) Data protection impact assessment on the processing of diagnostic data, https://www.government.nl/binaries/government/documenten/publications/2019/07/23/dpia-microsoft-office-365-online-and-mobile-slm-rijk-23-july/DPIA+Microsoft+Office+365+Online+and+Mobile+SLM+Rijk+23+july.pdf (24 Feb 2023).

[18] European Data Protection Board, 2022 Coordinated Enforcement Action - use of cloud-based services by the public sector, https://edpb.europa.eu/our-work-tools/our-documents/report/coordinated-enforcement-action-use-cloud-based-services-public_en (27 Jan 2023), p. 2, 24-26.

[19] E. de Graaf, G. J. Ritsema van Eck, 'Doorgiften van persoonsgegevens naar de VS post-Schrems: een empirisch onderzoek naar bedrijven die ook maar wat doen', *AA* 2023, afl. 1, p. 9-16.

[20] For individual cases there are also further exemptions. For more details see O. J. Gstrein, A. Zwitter, 'Extraterritorial application of the GDPR: promoting European values or power?', *Internet Policy Review Volume* 2020, afl. 10 – 3, p. 11-13.

relate to very basic requirements of data protection law, which must be in place for the legal framework to function in the first place. There seems to be a fundamental power imbalance when it comes to the negotiation of contracts and clarification of roles. At the same time, there seems to be a lack of transparency and understanding of what is going on. It is unclear if, when, to whom, and for which purposes personal and telemetry data flow as they are being analysed, stored, and potentially re-shared in various forms.

However, one might argue that the use of personal data inherently comes with risks that require mitigation, and that the hypothetical chance to re-identify a person is hardly ever zero.[21] Legal, organisational, and technical measures can be taken to get formal guarantees and oblige cloud service providers to do what is feasible to minimise privacy-related risks. Finally, it seems entirely unrealistic to stop the use of cloud-services and storage as such, and ultimately the risks relating to the individual might not be too concerning for many anyways. The efficiency and convenience gains of using cloud-services seem to simply outweigh the principled considerations and potential risks described, especially for most 'regular users' and organisations who 'have nothing to hide'.[22] Still, when looking at the bigger picture it turns out that data protection and individual privacy in a traditional sense are not able to capture the entire dimension of the issue. Rather, too much focus on these relevant aspects might distract and lead to a tendency to micro-manage and search for quick formalistic fixes.

3. What is Data Autonomy?

The persistent sharing of large amounts of information that characterises cloud-computing results in the requirements that the parties involved can be trusted, act reliably, and in a predictable way over a longer period. Eventually, there needs to be a set of shared values and

[21] M. Finck, F. Pallas, 'They who must not be identified—distinguishing personal from non-personal data under the GDPR', *International Data Privacy Law* 2020, afl. 10 – 1, p. 11–36.

[22] On the fatality of this argument see Solove, D.J. 'I' 've got nothing to hide and other misunderstandings of privacy', San Diego L. Rev., 2007.

principles, governing such (cross-border) data flows to create reliability.[23] This might be the shared belief in a democratic political system which requires autonomous actors,[24] respect for the rule of law, or the support and protection of human rights such as privacy, freedom of expression, and academic freedom. While such a commitment might undermine efficiency and economic gain in the short term - since it limits the number of potential partners - it introduces the checks and balances needed to guarantee that all actors involved remain with some space for deliberation, (dis)agreement,[25] and action.

As already mentioned in the introduction, in its broadest sense data autonomy can be defined as the capacity to make meaningful decisions about data. From an individual perspective, it can be understood by referring to the concept of 'informational self-determination', which is a constitutional right developed in (West-)Germany in 1983.[26] Different from privacy and data protection, informational self-determination is based on the idea of preserving human dignity and enabling personal development by giving the citizens of a state the right not to be afraid of what the state could know about them.[27]

Data autonomy as a concept builds on this understanding, but expands it in three dimensions. First, informational self-determination is focused on the relationship between a citizen and a

[23] J. Hildén, 'Mitigating the risk of US surveillance for public sector services in the cloud', *Internet Policy Review* 2021, DOI: 10.14763/2021.3.1578, p. 17-18; A. Baur, 'European Dreams of the Cloud: Imagining Innovation and Political Control', *Geopolitics* 2023, DOI: 10.1080/14650045.2022.2151902, p. 19-21. Science Guide, 'SURF waakt voor afhankelijkheid van uitgevers en big tech-bedrijven', https://www.scienceguide.nl/2022/02/surf/ (1 Feb 2023).

[24] For the connection between privacy and autonomy as a pre-requisite for democracy see T. Stahl, 'Privatheitsrechte und politische Öffentlichkeit', in H. Behrendt et al. (red.), *Privatsphäre 4.0 Eine Neuverortung des Privaten im Zeitalter der Digitalisierun*g, London: Springer Nature 2019, p. 123-139.

[25] In this context see L. Taylor, 'Can AI governance be progressive? Group interests, group privacy and abnormal justice', in: A. Zwitter, O.J. Gstrein (eds.), *Handbook on the Politics and Governance of Big Data and Artificial Intelligence*, Cheltenham – UK, forthcoming June 2023.

[26] For a monograph on the subject see M. Albers, *Informationelle Selbstbestimmung,* Baden-Baden: Nomos, 2005.

[27] O.J. Gstrein, A. Beaulieu, 'How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches', *Philosophy & Technology* 2022, afl. 35 - 3, p. 23-24.

state. In contrast, data autonomy also involves the relationship between private actors, especially in cases of stark power imbalances between contracting parties. Secondly, data autonomy is not limited to individual rights and duties. It includes organisational autonomy as an enabler for individual autonomy, similarly to the way that academic freedom entails both institutional and individual guarantees. Thirdly, data autonomy is not limited to mitigation of risks resulting on insights based on existing and recorded data (e.g. data stored in data bases). The emerging capabilities of Big Data infrastructures, coupled with machine learning and AI technologies enable the prediction of the likelihood of future events, as well as the generation of inferences indicating personal capabilities, beliefs, and preferences.[28] The sheer existence of these data-generated assumptions might undermine the possibility to make choices in the future, and therefore limit autonomy.[29]

4. Why you should care

The question remains why exactly this dependency on cloud infrastructures is concerning. After all, the use of cloud infrastructures provides convenience, is efficient, and typically more reliable than other options. Another important aspect is the user experience, which is typically smoother and more consumer-oriented when compared to services hosted by local IT-departments with limited resources. Since the scope of this contribution is limited, the focus in this section will be on two arguments why the dependency on cloud infrastructures is nonetheless concerning.

4.1. Lack of Exit-Strategy

One of the easiest ways to understand the profound and problematic dependency is to consider the options for exit-strategies. If universities were to stop the use of cloud services offered by companies such as Amazon, Google, or Microsoft all together, which alternatives

[28] S. Wachter, B. Mittelstadt, 'A right to reasonable inferences: Re-thinking data protection law in the age of Big Data and AI', *Columbia Business Law Review* 2019, p. 502-517.

[29] On the limitation and necessity to make such choices to promote human dignity see L. Floridi, 'On Human Dignity as a Foundation for the Right to Privacy', *Philosophy & Technology* 2016, afl. 29.

are there? One might think of a profound switch to open-source environments, but similar projects in other parts of public administration – such as the city of Munich with its ambitious LiMux project started in 2004 – struggled for decades before eventually switching to and remaining with a big tech company.[30] At the same time, projects to pool resources and create a 'European cloud' (e.g. Gaia-X) are in their infancy with slow progress.[31] One of the big challenges they face is to answer the question what specifically makes a cloud 'European', while avoiding the pitfalls of political populism/nationalism, or economic protectionism.[32] There might be some exceptional examples of universities which implement Open-Source software and services based on a broader strategy,[33] coupled with the call of academics such as Dobusch to increase the use of the 'Fediverse' with its decentralised services such as Mastodon.[34] However, by and large the lack of user literacy and experience, as well as questions around the maintenance and cost structure usually undermine such efforts.

This calculation might change if one considers the situation more broadly. A fundamental lack of ability to make meaningful choices about data is simply not compatible with academic freedom. Applying a republican understanding,[35] one can understand political liberty and

[30] Münchener IT-Referentin: Kein zurück zu LiMux, aber Open Source stärken, heise online, https://www.heise.de/news/Neue-IT-Referentin-in-Muenchen-Kein-zurueck-zu-LiMux-aber-Open-Source-staerken-7191854.html (2 Feb 2023).

[31] A. Baur, 'European Dreams of the Cloud: Imagining Innovation and Political Control', *Geopolitics* 2023, DOI: 10.1080/14650045.2022.2151902, p. 19-21. To find out more about Gaia-X go to https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html (2 Feb 2023).

[32] This is often labelled as a discussion about 'Digital sovereignty'. More information on the concept can be found at J. Phole, T. Thiel, 'Digital sovereignty', *Internet Policy Review* 2020, afl. 9 - 4, DOI: 10.14763/2020.4.1532.

[33] Zusammenarbeit: MS Teams als Lockangebot in eine geschlossene Microsoft-Umgebung, heise online, https://www.heise.de/news/Zusammenarbeit-MS-Teams-als-Lockangebot-in-eine-geschlossene-Microsoft-Umgebung-6030514.html (2 Feb 2023).

[34] L. Dobusch, Hochschulen aller Länder ins Fediverse!, https://netzpolitik.org/2023/aufruf-hochschulen-aller-laender-ins-fediverse/ (24 Feb 2023).

[35] A similar argument has been proposed by Titus Stahl, during an event on Data Autonomy hosted by the Center for Information Technology at the University of Groningen, held on 28 Jun 2022.

autonomy as being free from dominance.[36] A classic example is the situation of a group of slaves, who have a well-meaning master. While the slaves might be generally satisfied with their situation and institutional protection, there can be no doubt that they remain unfree and that their choices are fundamentally limited. In contrast, a positive conception of liberty in a republican sense results in self-mastery – or full autonomy – and the ability to define one's circumstances. Here the actors can do what they desire, since there is no institutional framing, no dominance, but also no protection.

Certainly, in effect the distinction between these two types of liberty is not straight-forward. Even individuals and institutions that could be seen as free in the positive sense will have to co-operate with others, which limits their liberty and autonomy. Yet the question remains about the ability to choose in the first place, the dependency on the choices of others, and whether any choice essentially matters in the sense that it has an impact on the strategic positions of the main actors involved in the decision-making process.

4.2. Data exploitation, training data and inferences

One of the main concerns of IT-professionals at universities is that it becomes increasingly challenging to separate data storage from the use of certain applications. Cloud environments increasingly merge tools, features, and data, which makes the customer ever more dependent on the provider ('vendor lock-in').[37] In essence, the longer that the data stays with a certain provider, and the larger that a data set becomes, the more power transfers from the sphere of the client to the sphere of the service provider. The fundamental questions and choices on what happens with the data remain with the infrastructure provider, while the user remains focused – and limited – on the 'cloud user experience'. This is a result from the possession and control of the infrastructure of the provider, and somehow ironic since most of the labour needed to create the data comes mostly from the side of the user. From a data protection

[36] Republicanism, Stanford Encyclopedia of Philosophy, https://plato.stanford.edu/entries/republicanism/ (2 Feb 2023).

[37] B. Satzger, W. Hummer, C. Inziger et al., 'Winds of Change: From Vendor Lock-In to the Meta Cloud', *IEEE Internet Computing* 2013, p. 69.

law perspective, the contrast is even more stark: the user/client remains the data controller who is essentially responsible for personal data collected and processed, whereas the cloud service provider is typically a processor with a focus on providing technical capabilities and a safe environment. This raises the question how limited the users are to remain with one cloud service provider. While there are European initiatives in data protection law and other legislative frameworks to facilitate the migration of data between services,[38] practice shows that such a migration is typically very costly and difficult to organise without standardised procedures between providers. Equally big is the challenge to migrate users, who are used to a certain set of applications, features, and workflow.

Once the data is part of a certain infrastructure, it can also be used to train models and create aggregated insights. This might be beneficial for the improvement of the services themselves. For instance, how might an already powerful language model such as ChatGPT evolve as it becomes part of Microsoft Teams or the search engine Bing, with the ability to interact in real-time with its hundreds of millions of users, including at universities?[39] Or to put it in a more provocative question: How many academic articles does one need to 'feed' into ChatGPT, so that it is able to write an assignment for students to pass all written exams three years from now? Nobody knows the answer to this question exactly, but we will certainly find out.

Last but not least, cloud providers can analyse the stored data in an aggregated way to generate insights on new developments in certain areas of research, administrative practices, or interesting topics for people working in higher education. Even if such analysis is not focusing on the individual user level, the results could be valuable to identify trends and gain insights on the populations of students, lecturers, researchers and administrative staff. Potentially such insights could be very useful, but who will benefit from them and under which

[38] J. Svoboda, 'Public Procurement and Vendor Lock-in within the Area of Data Migration', *Milan Law Review* 2022, afl. 3 - 1.

[39] Microsoft integriert Chat GPT in Teams und startet Premium-Abonnement, Derstandard.at, https://www.derstandard.de/story/2000143151939/microsoft-startet-teams-premium-und-integriert-chatgpt (2 Feb 2023). Microsoft's ChatGPT-powered Bing is open for everyone to try starting today, The Verge, https://www.theverge.com/2023/2/7/23589587/microsoft-chatgpt-bing-ai-event-preview (12 Feb 2023).

terms? One worrying example in this context is the changing role of actors such as publisher Elsevier, who increasingly collects data (e.g. academic articles, datasets) through online databases such as PURE to increase profit, as well as the influence in scientific publishing.[40]

5. Conclusion

In this discussion, we cannot be pragmatic. We must demand to keep principles and values in focus. What are the necessary preconditions for a data infrastructure that respects, protects and promotes academic freedom, enables free expression and critical thinking? There are no easy fixes, and no short-term solutions that solve this fundamental question. The more universities profit from high-speed connectivity and increased capabilities to measure, observe and find information, the more urgent it is for them to have a sizeable stake in shaping the datafication of society. To date it is mostly consumer mindsets that pave the way for this paradigmatic shift. Accordingly, corporate providers increase their influence, as long as they provide a good customer experience. Universities – just as consumers – desire services that are easy to use, perfectly maintained, and highly reliable. At the same time, they are not prepared to pay for this essential infrastructure, let alone develop, build, and maintain it to a significant extent themselves. When we consider that we need data infrastructure to study, teach, and research today more than a roof over our heads, is such an approach realistic? Without a profound discourse and detailed clarification of the underpinning values and rules for this new environment, higher education becomes increasingly dependent on the choices of others.

[40] F. van Heest, Open Access levert Elsevier steeds meer winst op, https://www.scienceguide.nl/2023/02/open-access-levert-elsevier-steeds-meer-winst-op/ (24 Feb 2023).