Governing the ‘datafied’ school: Bridging the divergence between universal education and student autonomy

By Theresa Henne* & Oskar J. Gstrein†

* Research Associate at the Department of Innovation and Digitalisation in Law, University of Vienna, Austria

† Programme Director BSc Data Science & Society, Assistant Professor Governance and Innovation, Member Data Research Centre, University of Groningen, Netherlands

Version 27 June 2022

Accepted for publication in ‘Handbook on the Politics and Governance of Big Data and Artificial Intelligence - Elgar Handbooks in Political Science series - edited by Andrej Zwitter & Oskar J. Gstrein, 2023.’ Please consult the volume for final corrections and page numbers.

Abstract

Students and teachers find themselves increasingly surrounded by Big Data and AI technologies that facilitate the learning process and the organisation of school life. Accordingly, vast amounts of data are being collected on the working of the entire school community. This trend--referred to as the ‘datafication’ of education--was pushed immensely during the COVID-19 pandemic. However, already before the necessity to quickly find digital solutions for remote teaching and learning, many scholars were concerned about the privacy and autonomy of the ‘datafied’ student and the corresponding larger effects on public education and democracy as such. In this chapter, we approach the datafication of school education through the lens of data protection and autonomy. We point to the inadequacies in the European data protection framework, which is considered as the state of the art by many. In search of other capable legal concepts, we explore the German ‘right to informational self-determination’, which introduces the distinct argument that restricting data flows is a necessity for the free personal development of the individual--a notion relevant for the tumbling, ever evolving minds of children and teenagers. We find that the fuzzy realities of school life demand a nuanced governance approach that balances individual control and privacy protection with the interests, needs and visions of the school community.

Keywords – GDPR, EdTech, Informational self-determination, Human Dignity, School, COVID-19
1. Introduction

The COVID-19 pandemic affected many sectors of society in unforeseen and profound ways. Among them is the educational sector, which experienced an amplification of trends that remained on the backburner for some time. Certainly, enhanced data collection and connectivity in the context of personalised learning and school management, the use of Big Data infrastructure to train ‘smart algorithms’ and ‘artificial intelligence’ (AI), as well as the implementation of emerging technologies such as mixed/virtual/augmented reality in educational concepts have been discussed for decades now.\(^1\) However, the pandemic has drastically and rapidly increased demand for such services and applications - typically referred to as ‘edtech’ or ‘edutech’. They are now used in ever growing numbers by school and university students, parents and teachers all across the world.\(^2\) The sudden urgency to provide education at scale over distance, combined with the difficulty for most (public) schools to do so instantly and effectively can be seen as the result of the inability (or unwillingness?) of educational institutions to address seemingly unavoidable trends.\(^3\) At the same time, the economic interest from the private sector in edtech grows, with one report valuing the market at around USD 85 Billion in 2021 with an expectation to grow up to USD 218 billion by 2027.\(^4\)

In this chapter we consider how the datafication of schools is being shaped through emerging Big Data and AI infrastructures and investigate the situation of students in Germany during the year 2021. We focus on how this transformation affects the personal development of students as they develop from kids into teenagers and young adults. We analyse and discuss the datafication of schools in relation to privacy, data protection, as well as personal development which we approach through the lens of ‘informational self-determination’. Whereas privacy and data protection are widely established in legal frameworks, it is particular to Germany that also informational self-determination has a formal status as a legally binding fundamental


right. It is because of this unique legal framework and the high socio-economic status that we chose Germany as the field of study.\textsuperscript{5}

In the context of this chapter, we consider how aforementioned individual rights, governance principles and legal guarantees apply to minors in primary and secondary education. As more and more data on the learning processes and administrative practices in schools are generated, one would expect that legal frameworks such as privacy and data protection laws, or associated constitutional rights safeguard the autonomous space of children and their families. Through such protection they would allow and encourage students to become critical and independent citizens, capable of making meaningful decisions for democratic societies.

However, as we argue based on the analysis below, the existing governance approach in a seemingly advanced democratic country such as Germany lacks effective safeguards and remedies for minors. Especially the current generation of students is going through an educational process that is more data-dependent than ever before and the effects on the future personal development of students might be particularly severe if the process of datafication starts at such a young age. The diverse landscape of educational institutions is increasingly populated by private, semi-private and international schools, which too a smaller degree are subject to state regulation.\textsuperscript{6} Furthermore, many of the concerns raised in this chapter will likewise be applicable to data processing in higher education, which, however, differs in regard to that most data subjects are no longer minors. The focus of this chapter, however, solely lies on public schools in primary and secondary education.

2. What is potentially lost with datafication of schools?

The COVID-19 pandemic forced schools all over the world and in Germany to shift to remote home schooling or hybrid classroom formats.\textsuperscript{7} This need for rapid adaptation once more exposed the existing global inequalities in public education.\textsuperscript{8} Where possible, the inadequacies were sought to be levelled out by investments in hard- and software, that alongside facilitating teaching and learning gathered data
on students and the entire school community. Whereas some authors frame the pandemic as a long-overdue momentum to catch-up with digital forerunners, such as Singapore, Denmark or Sweden, others fear the consequences of ad-hoc digitalisation and the increasing influence of private players in public education. Already before the pandemic educators and academics raised concerns on the effects of datafication on the privacy and autonomy of students, as well as the educational system as a whole.

Besides real-time monitoring of the cognitive activities of students, an abundance of other data types, such as demographics, physiological and emotion metrics, or social media activities, are explored for assessing the knowledge of students, their skills and learning patterns, as well as for improving their health and wellbeing. These trends are likely to increase with the introduction of augmented, mixed- and virtual reality devices in classrooms, which can offer even more behavioural data.

The generated data can be modelled into ‘data doubles’ or ‘digital twins’ of students, which might act as a basis for categorizing their abilities and individual character. This makes predictions on their future behaviour and potentials possible, which might result in recommending certain pathways in education or employment while discouraging others. If such categorizations and predictions are based on immature and hardly tested technology, incomplete or biased data sets, or are applied uncritically, they severely limit the potential for personal development of the students concerned. The models, which underpin the response of institutions and which define what is considered a ‘successful’ student, are regularly untransparent and opaque. Often student data is masked as an objective truth ignoring its

---

15 Jones and McCoy (n 13); Williamson (n 11).
16 Broughan and Prinsloo (n 14).
political, inherently incomplete and often erroneous nature. Jones argues that ‘[e]ven with noble and good ends in mind—namely improving learning (however defined)—’, the surveillance and intervention in the life of students undermine their agency and voice, whereas it should be the purpose of public education to nurture it.

Next to the invasion of the privacy of minors that comes with the exploitation of individuals as data sources, critics also point to the effects of datafication of students on public education and democracy. The logics of datafication, personalisation and commodification, which already govern large parts of society as Van Dijck illustrates, also threaten to permeate a public education that ‘has long been one of the most precious common goods and the backbone of Western democracies’. With private companies entering the educational spheres, the privilege of the state to govern what and how students learn may be challenged by commercial interests. Public education or ‘Bildung’ (loosely formation) builds on the pedagogic qualities and autonomy of the teacher, the social momentum of learning and the discovery that making mistakes is part of self-development. Certainly, the personal development of the individual has also been guided in traditional settings of education by the teachers and the learning environment. It is the task of educational institutions to expose students to thoughts, objects and practices that they would not encounter through their families, friends, or algorithmic predictions.

---

17 Jones and McCoy (n 13); Sharon Slade and Paul Prinsloo, ‘Learning Analytics: Ethical Issues and Dilemmas’ (2013) 57 American Behavioral Scientist 1510.
19 Livingstone, Stoilova and Nandagiri (n 18).
23 Lupton and Williamson (n 12).
and inspire them to pick up professions and hobbies. Still, ultimately it is the mind of the student, which combines and assesses all of these influences and decides which interests to pursue.

Through the lens of enlightenment, the purpose of education is to transform students into autonomous citizens on their way in life and society—along the notion of Immanuel Kant’s famous quote ‘sapere aude’ or ‘have courage to use your own reason’. These values are considered at threat with the introduction of technology that transforms people and their practices into data and monitors them permanently while constantly extrapolating potential paths of thinking and action. This also coincides with a style of teaching that cuts education into (micro-)learning units, that aims at optimizing the skills of a future workforce (‘human capital’), rather than treating students as future citizens with curious minds and maturing characters. If ‘individualised’ learning comes down to using the personal data insights for means of nudging a student into what is considered an optimising behaviour, the individual right to personal development and the opportunity to have a free and informed opinion are lost in public education.

When investigating the realities of German schools as elaborated in section 4, images such as Williamson’s ‘dataveillance school’, in which children are reduced to a calculable actor and judged upon their data doubles, seem not to fit the perception of local actors. Also, the notion of public schools as spaces of surveillance and social control is certainly not a new idea. Foucault, Deleuze and others have highlighted and discussed this function long before the emergence of Big Data and AI. Yet, only a look at documented cases in countries such as the United Kingdom, France, Sweden or Bulgaria is required to understand that invasive technologies such as facial recognition are already deployed at scale in schools. Corporations such as Intel are increasingly exploring this space, promising to be able to detect student emotions remotely using machine learning. Without meaning to reproduce the alarmist tone that commonly accompanies most discussions in Germany involving ‘big data’, ‘artificial

24 Watters (n 11).
25 Livingstone, Stoilova and Nandagiri (n 18); Jones, Rubel and LeClere (n 18).
26 Anne Beaulieu and Sabina Leonelli, Data and Society: A Critical Introduction (SAGE Publications Ltd 2022); Jones and McCoy (n 13).
27 (n 11).
intelligence’ and ‘education’, we find evidence that raises questions about the direction that public education is heading when it comes to nurturing personal development, free thought and critical thinking. Yet there are indications that Germany’s educational landscape might differ from other countries, who already rely much more on Big Tech solutions and do not know the notion of informational self-determination. Hence, Germany might provide an exceptional space for developing ‘edTech’ and governance mechanisms that promote democratic values and counters exploitative data logics.

3. Framing the datafied school through data protection law and informational self-determination

In the following, we examine the existing legal privacy and data protection framework applicable to the data collection in German schools on a national level. Based on this legal analysis, we argue that the consideration of novel concepts is required to address the challenges of growing up in the digital age. To build on the status quo, we explore the potential of a conceptual reframing of the right to informational self-determination as a means of resistance to the harmful effects of datafication.

3.1. Specific Protection of Minors in the GDPR

A central piece of legislation within the German and European data governance framework is the 2016 GDPR, which is generally perceived as setting high standards for the protection of personal data worldwide. The universal scope of the regulation is likewise applicable to educational institutions and any third parties. The legal framework for public educational institutions and private entities, such as edtech companies, nevertheless differs regarding the purposes they commonly pursue. Data processing that is performed for a public interest, such as providing universal education, justifies greater interferences with individual rights. However, according to the GDPR an additional EU or national law is required to define the public interest. Commercial interests can be pursued by relying for instance on the legitimate interest provisions under Art.6 (1) lit f, yet must be carefully balanced with the rights and freedoms of the data subject. Regularly, however, the different interests mix—for instance, when a private company is tasked by a school to process the data of students to provide (digital) services to them. Commonly the responsibility for the data processing remains with the educational institutions in

32 This includes the caveat that we exclude the sixteen federal school laws of German states since they would exceed the scope of this paper and seem not relevant to draw the main conclusions.
such instances, which is considered the data controller, whereas the third party processes such data within the bounds of the terms and conditions defined by the school. Although the GDPR adopts a principle based and technology neutral approach that includes a set of measures to restrict the scope of collection and use of personal data--e.g. necessity of valid legal basis before using data, transparency, purpose limitation or data minimisation--the regulation is also subject to criticism. For instance, Purtova admonishes that comprehensive data protection law in a datafied society will make it ‘the law of everything’, with practically no real-life situation imaginable where the regulation is not applicable.

Whereas the 1995 EU Data Protection Directive 95/46 EC that preceded the GDPR did not entail a single notion indicating the necessity of special treatment of the personal data of minors, the GDPR contains some improvements. Recital 38 serves as a starting point for this investigation since it provides insights into the reasoning why minors should be treated differently than adults. It is argued that their personal data should be subject to specific protection measures because children ‘may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.’

Hence, the GDPR fails to recognise that children require specific protection not only because their capacity to exercise reason is immature but more so because child- and teenagerhood is a sensitive and formative phase. Data harms occurring at a young age might be particular severe and might interfere in the personal development of the child more profoundly than in adulthood. Justifying specific data protection measures only based on the cognitive immaturity of minors misses to address the more significant objective, namely to establish extended safeguards against the invasions of privacy and autonomy and for the protection of personal development.

Building on a lacking problem analysis, the proposed measures of the GDPR are far from satisfactory. We begin with outlining the GDPR’s primary response to the identified vulnerability of children, namely to limit the legal bases on which the data of minors can be processed, followed by a discussion on the relevance of the right to erasure (‘right to be forgotten’), child-friendly transparency requirements and automated decision-making.

3.1.1. Legal basis for processing personal data

Personal data processing under the GDPR must be based on one of six legal bases listed in Art 6 (1), of which four remain indifferent to the age of the data subject. If personal data is processed for the implementation of a contract, compliance with a legal obligation, protection of the vital interest of the

---

data subject or the performance of a task in public interest, data controllers do not need to adhere to any further restrictions in cases where the data of minors is involved.35

In order to justify in accordance with Art. 6 (1) lit e that the processing necessary for the performance of a task carried out in the public interest the respective tasks must be laid down by a EU or national law, as Art. 6 (3) states. The respective federal German state laws on data processing in educational institutions--despite a few exemptions--do not explicitly cover data collection beyond the name, address and grades of students. The federal state of Berlin, however, reformed their educational law in 2021 so it incorporates data processing by the school for the purpose of using digital teaching and learning tools insofar as this is necessary for the fulfilment of their educational mandate.36 In most other federal states legal uncertainty remains regarding which legal basis schools refer to when cooperating with edtech companies.

Another potential legal basis that edtech companies can rely on when processing student data is the legitimate interest provision in Art 6 (1) lit f. However, data processing based on the legitimate interest of the data controller (or another third party) can be overridden by the interests, fundamental rights, and freedoms of the data subject--‘in particular where the data subject is a child’. Hence, the proportionality of the interference must be carefully weighed against the rights of the children that result from potential data harms.37 Still, it remains unclear under which conditions an edtech provider can rely on the legitimate interest provision for processing data. Given that students will hardly expect that data collected in the classroom is used for purposes outside of the educational context, it is highly questionable whether the legitimate interest of a private company to develop their technology or market their products outweighs the rights of the child.

Furthermore, referring to the most prominently applied legal basis for data processing38—the consent of the data subject—is limited in cases where the data subject is a child. Art 8 (1) of the GDPR states that where ‘information society services’ are offered to a child directly,39 the data subject must reach the

---

38 According to Kess and Nagel, the leading doctrine says that not only services that do not exclusively target children fall under Art 8 (1) but also so-called “dual-use” services such as WhatsApp or Instagram that are likewise used by adults and children.
age of 16 years for being able to agree to the processing based on Art 6 (1) lit a. Children below the age of 16 rely on their parents to provide consent on their behalf. National member states, however, may with national law lower the age for consent down to 13 years. In practice, this leads to a scattered GDPR data landscape when it comes to the age required to provide legitimate consent. At the end of 2019 nine (of the then 28) EU member states required a minimum age of 13 for consent, six an age of 14, three an age of 15 and ten the age of 16.\footnote{Ingrida Milkaite and Eva Lievens, ‘Status Quo Regarding the Child’s Article 8 GDPR Age of Consent for Data Processing across the EU’ (BIK Portal, 20 December 2019) <https://www.betterinternetforkids.eu/practice/awareness/article> accessed 24 March 2022.} In the context of datafied education the age limitation for consent will regularly exclude students from making related decisions, who instead rely on their parents to agree or disagree with processing of their data.

Furthermore, the immense informational burden coming with the scale and complexity of the data economy makes it impossible for the individual to assess the risks and consequences of the data processing that they shall agree to.\footnote{Daniel J Solove, ‘Privacy Self-Management and the Consent Dilemma’ <https://papers.ssrn.com/abstract=2171018> accessed 13 February 2022.} Hence, the condition of lacking cognitive capacity, which Recital 38 attributes to children and based on which it justifies the limitation of their right to consent, can likewise be diagnosed among adults. Consequently, transferring the responsibility for assessing the risk of data processing to the legal guardians of a child will often not lead to adequate protection of the child. Rather, it might worsen the situation since parents who already struggle with managing their own data flows will likely react with practical indifference due to informational overload--and agree to terms without considering potential data harms.\footnote{I van Ooijen and Helen a U Vrabec, ‘Does the GDPR Enhance Consumers’ Control over Personal Data? An Analysis from a Behavioural Perspective’ (2019) 42 Journal of Consumer Policy 91; F J Zuiderveen Borgesius and others, ‘Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the EPrivacy Regulation’ (2017) 3 European Data Protection Law Review 353.}

Corresponding to the criticism outlined above, Buitelaar points to the lack of empirical evidence that people over the age of 16 are more capable of overseeing the risks relating to their personal data.\footnote{Livingstone, Stoilova and Nandagiri (n 20); Buitelaar (n 20).} It is therefore questionable why 16-year-olds should be expected to make good decisions from this age onwards, in particular since the vast majority of EU member states only grants full legal capacity at the age of 18 years.\footnote{European Union Agency for Fundamental Rights, ‘Age of Majority’ (12 November 2017) <https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements/age-majority> accessed 28 February 2022; Buitelaar (n 20).} Buitelaar further criticises the GDPR age limitation regime as an ‘on-off approach’ that does not sufficiently consider ‘the evolving capacities of the child’. The latter is introduced as legal
concept in the Convention on the Rights of the Child (CRC) and encourages parents to involve children in (co-)determining their life with respect to their development.45

3.1.2. The Right to Be Forgotten as a remedy for minors

Article 17 GDPR stipulates an individual right to demand erasure of personal data. The provision is also commonly referred to as the ‘right to be forgotten’, although this is not entirely accurate and requires more nuance.46 Article 17 GDPR contains several conditions to erase personal data of which one specifically refers to children.47 According to Art 17 (1) lit f GDPR in combination with Art 8 (1) GDPR a data subject may withdraw consent that has initially been given by their parents. Unfortunately, this provision is rather vague. It is not further clarified whether the child itself must reach the age for legally providing consent for making use of it. However, given that otherwise Art 17 (1) lit f GDPR would be conflicting with the authority granted to legal guardians in Art 8 (1) GDPR, the same age limitation must be assumed for demanding erasure. Therefore, this facet of the right seems drafted as a remedy for minors who disagree with past decisions of legal guardians such as parents. Recital 65 of the regulation further clarifies that the right to erasure is also relevant in cases where a minor was legally allowed to give consent--sometimes as early as at the age of 13--but was not fully aware of the potential harms involved when agreeing to the data collection and processing. Hence, Recital 65 recognizes that despite the age limitation, children might still be put into the position of making unsafe choices. However, whether retrospective deletion of personal data can be considered as satisfactory remedy for the diverse harms potentially stemming from data collection and processing is questionable. Frequently, it will be neither apparent to minors (or their legal guardians) how data trails might result in harm over a longer period.48 Furthermore, these types of harms are not easily revisable or reparable once they occur. To make this more concrete just with two examples, one can only speculate how the data trails of minors impact future choices of educational institutions, or potential employers who increasingly use

45 (n 20).
46 Gstrein (n 33) 125–127.
AI tools to create personality profiles of their applicants? Finally, the debate about material compensation for infringements of GDPR data protection rights is active, but still in its infancy.

3.1.3. Review of child-friendly transparency & automated (faulty) decisions

The principle of transparency, which is enshrined in Art 5 GDPR and fundamental for several rights of data subjects, is another GDPR mechanism that acknowledges child-specific needs. According to Art 12 GDPR information on data processing must be provided ‘in a concise, transparent, intelligible, and easily accessible form, using clear and plain language’. This applies according to the Art 12 to any information addressed to a child in particular. In practice, child-friendly transparency, however, is rarely provided. Based on the investigation of the privacy policies of Instagram, Snapchat and TikTok Milkaite concludes that such policies are still largely text-based and complex. More effort needs to be taken to develop child-specific communication formats. In the empirical analysis in section 4, we conclude that the stakeholders of public schools likewise struggle to provide students with sufficient transparency. Again, the discussion on child-specific measures mirrors a broader debate on the dilemma between not overwhelming the audience with information while at the same time not over-simplifying the terms and conditions of the data processing agreements.

Closely related with the notion of transparency is the right not to be subject to a decision based solely on automated processing of personal data that produces legal or similarly significantly affects in Art 22 GDPR. Sometimes this is also being referred to as a right to human review or explanation of automated decisions ‘made by algorithms’. However, the academic discussion on the precise scope, meaning and practical feasibility of this provision is still lively and ongoing. The language of the regulation has been criticised as being overly vague. It is not entirely clear who needs to explain what to whom, in which detail, when and how. More questions can be raised around multi-staged decision-making processes, where different groups of humans closely interact with complex data models at different stages of a problem analysis and strategy development. Given, however, that the decisions made by automated systems in the educational context, e.g. for grading, providing feedback or recommending learning

51 Milkaite and others (n 20).
52 ibid.
53 Solove (n 41).
54 Barros Vale and Zanfir-Fortuna (n 29).
pathways, might have significant effects on the future pathway of an individual, it is of utmost importance to enable young people to understand, evaluate and challenge the output of such systems.

To summarize, the constructional flaws of informed consent, the resulting inadequacy of transferring consent rights to the legal guardian, the insufficiency of the right to erasure/be ‘forgotten’ to act as a remedy for data exposure, the lacking implementation of child-friendly transparency standards, as well as the unclear notion of what it means to review/explain automated-decisions broadly undermine the attempts of the GDPR to provide specific protection to children. This is not to say that the GDPR leaves minors without protection, since most of the requirements and safeguards of the regulation are applicable to the processing of personal data regardless of the age of the data subject. However, the GDPR fails to provide child-specific protection, despite the good intentions mentioned in Recital 38.

Whereas currently, the primary response of the regulation to the vulnerability of children is to limit the legal bases on which their data can be processed, general requirements or limitations for processing the data of minors may be equally or more effective. For instance, during the discussions for the adoption of a the Digital Service Act (DSA) the European Parliament adopted an amendment that prohibits online platforms from using personal data “for commercial purposes related to direct marketing, profiling and behaviourally targeted advertising of minors". At the same time, discussions in the EU are ongoing on the adoption of an Artificial Intelligence Act (AIA), where many applications relating to decisions being made in education (e.g. exam assessment) are labelled as high-risk and might therefore become subject to strict standardisation. How all of these policy initiatives affect datafication in schools over the longer term will be seen as the regulatory frameworks materialise.

3.2. Informational self-determination as additional concept to address datafication

Since the existing European governance framework faces substantial deficits in addressing the needs of minors, it is necessary to investigate the potential of other concepts. In the following, we introduce and examine the right to informational self-determination and its ability to address the risks of minors. In
particular, it seems promising to us since the right proposes a distinct rational for why data flows must be restricted, namely the protection of the development of personality.\footnote{René Mahieu, ‘The Right of Access to Personal Data: A Genealogy’ (2021) 2021 Technology and Regulation 62.}

To elaborate on the background of the right, the German Federal Constitutional Court established the right to informational self-determination in a famous ruling of 15 December 1983 on the Census Act (‘Volkszählungsurteil’).\footnote{Oskar J Gstrein and Anne Beaulieu, ‘How to Protect Privacy in a Datafied Society? A Presentation of Multiple Legal and Conceptual Approaches’ (2022) 35 Philosophy & Technology 3, 23–24; Urteil vom 15 Dezember 1983, 1 BvR 209/83 (Bundesverfassungsgericht).} At the time, the government of West Germany announced a large-scale census program to collect personal and household data. The formal objective was to inform planning decisions and policymaking, but the plan sparked concerns about the power relationship between citizens and their government. Considering the technological capabilities of the time from the perspective of today, the judgement of the court seems prophetic in outlining the threats to individual freedoms stemming from unlimited collection, storage, use and disclosure of personal data. For addressing the risks, the right to informational self-determination grants the individual, in principle, the authority of the disclosure and use of their data as well as general measures aiming at ‘keeping data flows limited, transparent, and geared towards what is necessary for a free and democratic society’.\footnote{Mahieu (n 61) 69.}

Conceptually, informational self-determination has many parallels to data protection, yet remains different with an objective that goes beyond the formal protection of personal data. It has a two-pronged origin, combining two constitutional guarantees enshrined in the first two articles of the German Basic Law (‘Grundgesetz’) that came into effect in 1949. First, ‘every person shall have the right to free development of his [sic] personality’ as enshrined in Art 2 (1) of the Basic Law. Secondly, ‘human dignity shall be inviolable’ as stated in Art 1 (1) of the Basic Law. In the census judgment from 1983 the court decided that such space of personal discretion must also exist in the informational sphere and is therefore not limited to the physical domain.\footnote{Volkszählungsurteil (n 62) 1.} The evolution of the traditional notion of privacy is a challenge for many jurisdictions as they try to apply and interpret them in the digital age.\footnote{Gstrein and Beaulieu (n 62) 10; 17–20.}

Another interesting consideration is whether and how this right applies to minors and their personal development. The original judgment from 1983 is not directly engaging with this question, but it can be argued that the right to informational self-determination applies to minors since the law on data

---

\footnote{Oskar J Gstrein and Anne Beaulieu, ‘How to Protect Privacy in a Datafied Society? A Presentation of Multiple Legal and Conceptual Approaches’ (2022) 35 Philosophy & Technology 3, 23–24; Urteil vom 15 Dezember 1983, 1 BvR 209/83 (Bundesverfassungsgericht).}
\footnote{Mahieu (n 61) 69.}
\footnote{Volkszählungsurteil (n 62) 1.}
\footnote{Gstrein and Beaulieu (n 62) 10; 17–20.}
collection during the 1983 census also required collection of data relating to their living circumstances (e.g. are they keeping a household, how many of them live in a household). 66

The right to informational self-determination has seen some development over the past decades. More recently, in two decisions from 2019 in relation to the right to be forgotten, 67 the judges re-interpreted informational self-determination to also include commercial exploitation of data along the lines of Zuboff’s surveillance capitalism. 68 This could be a new development in the history of informational self-determination, that expands it beyond the focus on state interference to establish a duty of the state to create an environment where also private parties amongst themselves guarantee the right. This could be particularly relevant where power asymmetries come into play, such as in relation to consumers and Big Tech firms, or students who must attend public or private schools which are increasingly datafied.

While such developments seem promising for those who lament the shortcomings of traditional data protection and privacy law in the context of datafied education, the question remains how informational self-determination can make a difference in practice. Critics such as Veil highlight that the concept has a metaphysical character that is almost impossible to grasp and translate into concrete practices. 69 Also, it is a very national concept which raises the question how relevant it could be beyond the territorial borders of Germany. Potentially, one could argue that it might also be transferrable to the entire EU, as Article 1 of the Charter of Fundamental Rights of the EU includes a legally binding commitment to human dignity—modelled after the German constitution. 70 Yet it is uncertain what the future of the right looks like, certainly internationally and beyond Europe.

4. Datafication of public education in Germany

The data collection of schools may have been a rather mundane and redundant affair for decades. It turned the magical process of ‘Bildung’ into a bureaucratic deed and allowed for a pre-selection of students for the labour market. The ‘datafication’ of public education, however, refers to processes which are not much older than 20 years and seem to redefine the profane everyday politics of student data. This process is closely intertwined with the introduction of digital devices and services in the classroom and in the homes of students. In the following, we have a closer look at Germany’s

66 Volkszählungsurteil (n 62) 8.
67 Gstrein (n 33) 136–139.
educational landscape, compare its state of digitalisation to international standards and outline the peculiarities of the federated system. The meta-observations are complemented by the empirical investigation of two use-cases, in which we explore the current data practices of two German schools and reflect upon the implication of the status-quo on students’ privacy, autonomy and personal development.

4.1. Meta-Observations: In 2021, German schools are still without Wi-Fi

The digitalisation of education in Germany was pushed forward in recent years by numerous public and private entities.\(^71\) Despite these efforts, Germany is generally regarded as a latecomer in terms of digital education. In a study that explored the readiness of OECD countries for remote education, Germany ranked generally low despite its socio-economic status.\(^72\) Little more than 30% of the German headmasters surveyed in 2018 indicated that their school had an effective online learning support platform. In contrast, in top-ranking countries such as Singapore or Denmark above 90% of schools were equipped to provide remote learning effectively. Concerning the question whether effective professional resources were available for teachers to learn how to use digital devices, Germany ranked third from the bottom indicating that such resources where only provided at 40% of the German schools.

Furthermore, also within the German education system great disparities exist when it comes to the ability to provide digital education.\(^73\) Those schools that are considered digital pioneers possess a high-performance infrastructure and digital strategy, whereas even the most fundamental resources are lacking in others. Despite the catalysing force of the pandemic, in 2021 not even half of German schools provided Wi-Fi to their students, and still more than 40% of them did not incorporate a learning management system into their infrastructure.

One explanation of this fragmented digital education landscape lies in the federal structure of Germany, which confers the educational sovereignty to the Länder (federal states). In a survey across the 16 German states concerning which learning platforms are used,\(^74\) the vast majority indicated that no unified learning management system was implemented across all schools. Rather, a variety of solutions was offered on a voluntary basis. For example, Bavaria provided the learning platform ‘mebis’ to schools.

---


72 OECD (n 9).


However, only 12.5% of the Bavarian students used it. At the beginning of the pandemic, some schools also used more mainstream solutions such as Microsoft Teams. However, due to heavy criticism from Federal data protection authorities, such as Hessen and Baden-Württemberg, the licenses were terminated.\textsuperscript{75} Still to date, the use of tools provided by US-based companies is discouraged, which is a consequence of the judgments of the Court of Justice of the EU in the Schrems cases.\textsuperscript{76} These fragmented governance approaches, the lack of basic internet infrastructure, as well as high data protection standards hamper the access to the German edtech market.\textsuperscript{77} In order to promote digitalisation, Förschle observes that since 2012, but in particular since 2016, a growing number of networks and initiatives have been formed that lobby for a transfer of educational competencies to the national level and facilitate the introduction of a common national (data) infrastructure.

To summarize, the federal states are relying on a mix of corporate and public solutions. There is lacking evidence concerning which solutions are implemented on school level, since no unified standards and requirements are defined on the national or federal level. To get a better understanding of the ‘situation on the ground’ we investigate the practices of two German schools in the following.

4.2. On the ground: Investigating data practices of two German schools

The research that informs the following sections was conducted in spring 2021. It aimed at gaining an insight into the data practices at German schools and the related perceptions of stakeholders to explore the potentials and risks of datafied public education. Therefore, four workshops have been organised, of which the first two, which aimed at mapping the data ecosystem of two use cases, are discussed below. The findings from two Multi-Stakeholder Workshops inviting a wider set of participants to reflect upon the status-quo of ‘student data’ and (desirable) future trajectories are presented in Section 4.3.

The two schools investigated as uses cases, namely the Universitätsschule (US) Dresden (grade 1-6) and the John Lennon Gymnasium (JLG) Berlin (grade 5-12), are considered as forerunners in terms of digitalisation. Both schools were awarded by the industry association Bitkom, which honours so-called ‘Smart Schools’ based on criteria such as digital infrastructure, digital teaching, training of educators, and the schools strategy and vision for a digital future.\textsuperscript{78} Correspondingly, the schools had incorporated


\textsuperscript{77} Förschler (n 71).

\textsuperscript{78} ‘Was ist eine Smart School? | Smart Schools’ <https://www.smart-school.de/de/Smart-School> accessed 8 March 2022.
learning management systems (LMS) and other software systems into their pedagogical concept already before the pandemic hit in March 2020. At the JLG Berlin the Norwegian LMS provider ‘ItsLearning’ facilitated the collection of the learning data of students. The US Dresden has the privilege of cooperating with the Technical University Dresden and a Czech company in developing a custom-made LMS that fits the needs of the school. Given the digital divide inside of Germany’s educational sector, the data infrastructure of many other German schools is far less developed than the one described in the following. Hence, these two use cases should not be understood as representing the average German school. Rather, they represent stakeholders that are driving present developments and whose experiences are key to manifest best-practices for the entire German school system.

In the two use cases investigated, next to the LMS the schools also employed software systems that served mainly administrative and organisational purposes--such as generating timetables, checking the attendance of students or providing information. In both use cases, learning data is generated when students interact with the LMS by accessing materials, completing tasks online or submitting assignments. In the future the school might consider applying AI-based techniques for analysing student data: ‘The data is great for use with AI, something to think about in five, six or seven years’. In general, the data practices of the two investigated schools entail basic monitoring, aggregation and visualisation of the learning process. The degree of automatization and personalisation of education in the use cases is limited. Rather than framing the current state as a missed opportunity or deficit, the empirical data indicates that in the two cases it was a deliberate decision of the stakeholders to employ certain technical elements and to refrain from using others. Clearly, the US Dresden had more possibilities to shape the technical infrastructure to their needs and pedagogical concept given that they are co-designers of their LMS. However, also the LMS It’sLearning provides the teacher at the JLG Berlin with a vast variety of choices for designing and supporting the learning process. Although the JLG has several years of experience with ItsLearning, it is pointed out that they only ‘use about 20 to 30 percent of the possibilities’. Furthermore, it was mentioned that although the teachers of the JLG wished to provide students with ‘their own space, [which they could use] to develop their media competence’, the school decided against using existing services such as ‘Google suits’ for this end, one of the prime reasons being data protection concerns.

However, it has also become clear from the workshops that both schools already invest substantial resources in managing and developing their digital infrastructure, and that their visions often conflict with the realities of school life, in which time and finances are chronically short. Considering the digital
divide in the educational system, many German schools will not have the privilege of fitting their data ecosystem to their needs and visions. Instead, teachers, students, and all other stakeholders of the school community will either work with a minimum of digitalisation, in which exercises are send via mail or WhatsApp and printed out by the students, or will accept whatever digital tools are provided to them irrespective of whether they enable a form of learning that they consider relevant. The space for shaping digitalisation will be scarce at many schools. Hence, it is even more important that the lessons learned from those schools who have such capacities are conveyed to benefit the entire school system.

4.3. Critical reflection: Balancing Privacy and Autonomy with Feasibility and Efficiency

A fundamental question concerning the politics of student data is what data types shall be collected to serve whose interests. The literature typically assumes a depiction of a data ecosystem that is mainly built around commercial and institutional interest and exploits students as passive data providers, resulting in calls for ‘student-centred approaches’, which allow individuals to take control of their data.82 These narratives suggest that schools are either a place of modern surveillance, or a site of empowerment and rights for students. However, neither of the two scenarios seems to fit the fuzzy realities of the daily school life, in which many more stakeholders than edtech companies and students meet.

The following continues to discuss the risk and potentials of student data building on empirical insights of two Multi-Stakeholder Workshops that were conducted in spring 2021. The workshops invited a wide group of stakeholders of public education: representatives of students from Berlin and Dresden, members of civil society, providers of edtech and learning platforms, as well as teachers, parents and researchers from the TU Dresden. A full list of the participants and a summary of the findings can be found in Annex 1.

Although the participants shared many of the concerns already raised in the datafication literature (see section 2), this did not result in the demand for providing more control to students or a demonisation of edtech. Rather, the accounts of the participants display the complexities that data flows in public education produce, and which serve the functioning of the educational apparatus. The following section highlights the risks to the privacy, autonomy and agency of students discussed in the multi-stakeholder workshops. Furthermore, the accounts of participants are depicted, which display the impediments to realising a data infrastructure in public education that respects the rights of minors and balances interests.

82 Broughan and Prinsloo (n 14); Jones and McCoy (n 13); Slade and Prinsloo (n 17).
The data derived from school is a valuable resource for a diverse set of objectives. The participants of the two workshops agreed that the data of school students is very sensitive. Therefore, they are facing a dilemma resulting from the tension that student data is insightful and useful for supporting the learning process on the one hand, while posing great risks to the autonomy and privacy of the minors on the other hand. For example, comprehensive tracking of the learning activities over longer periods can enable a deeper understanding of the learning patterns of minors and allows for ‘more meaningful’ formative assessment methods. At the same time, this activity can also provide sensitive insights into the private and family life of the monitored persons. A participating student representative recalls a case of a learning platform from Schleswig Holstein, which enabled teachers to see at what times a student had accessed a data file. The participant said students are afraid of becoming overly transparent to the teacher, who observes not only the result of an assignment, but also the process of the development, which the conditions of remote schooling made more difficult than usually.

Another participant, who is a teacher at the USD, notes that safe spaces are required to support the development of students holistically. Students should not be afraid of being monitored, but encouraged to experiment, act and speak freely. For this aim, the teacher argues, ‘anonymity or at least an exclusive digital space, to which parents, peers and learning facilitators have only limited access, can be important to support the development of the student’.  

The empirical accounts display that the use of student data, also for means beneficial to the minors, must be balanced with their developing autonomy, agency, and privacy. A pre-condition for weighing risks and potentials is a comprehensive understanding of which data types serve which objective and are relevant to whom within the data ecosystem of a school. This is an issue that still requires the attention of researchers, argues a participant who himself conducts research at the USD. In effect, student data might not be collected systematically or with a clear purpose, despite the sensitive nature of the data. Instead of first determining which data types are valuable for the student or for researchers, a participant from civil society states, simply the data that is most easily accessible is collected: ‘Currently the cart is put before the horse. At first, it is considered which data is available or could be collected and what can possibly be done with this data at some point in the future, although one should first be thinking about the objectives.’

---

83 „Da kann Anonymität, oder zumindest ein begrenzter, digitaler Raum wichtig sein, der nur begrenzt von Eltern, Lernbegleitern, Mitschülern zugänglich ist, um die Entwicklung des Schülers zu unterstützen”.

84 „Momentan wird das Pferd von hinten aufgezäumt. Es wird erst geschaut welche Daten man hat, bzw. man sammeln könnte und was man irgendwann mit diesen Daten machen kann. (...) Dabei sollte man vom Ziel her denken”.
A great concern to the participant was the sharing of student data with external entities outside of the school. A primary fear was that data is exploited for commercial interests and is assigned with a price. A student representative argues that ‘it is already hard to be accompanied in life by the final mark of the Abitur [end exam grade]. Such data, however, which is so comprehensive and outlines in detail how a person functions, must not be sold, especially not to employers.’ \(^{85}\) In both workshops, the groups highlighted the importance of the ‘right to be forgotten’, \(^{86}\) which in their understanding must ensure that students are free to decide which data points sustain over time. Past data must not lead to path dependencies and thereby limit the prospects of a student. Therefore, when data is shared with third parties, it must be safeguarded that personal data does not affect students negatively in their futures.

A participant, who himself develops edtech products, points out that currently the biggest concern of the German educational ministries is that student data is employed for personalised advertisement. Learning platforms that are employed in school could use the data to their advantage and target minors and their parents to offer personalised learning tools outside of the classroom: ‘Many learning providers have an additional, fee-based after-school offer. The fear is that information generated within the school setting will then be used to sell something to the parents. In the sense of ‘if you want your child to graduate from high school, then you have to make use of these after-school programs.’ \(^{87}\) Therefore, the edtech developer proposed that student data should only be shared with private third parties if they adhere to a number of principles, such as the prohibitions of using the data for advertisement or of matching the data with other data sets.

A strong consensus existed among the participants that public and private players must provide more transparency concerning the student data they collect. As showcased by the example from Schleswig-Holstein, knowing which data is collected and accessed by whom is a pre-condition for an inclusive discussion concerning the data practices within schools. Yet, despite the willingness to provide more transparency to students, participants working at the USD indicated that they simply did not see the available capacity to perform such task among the current members of the school community (e.g. teachers or IT-managers). ‘Although transparency is a right of the GDPR,’ the former data privacy officer

\(^{85}\) „Es ist schon schwer, dass einen sein Leben lang die Abiturnote begleitet. Aber solche Daten, die so umfangreich sind und so gut skizzieren, wie dieser Mensch funktioniert, dürfen nicht verkauft werden, insbesondere nicht an Arbeitgeber”.

\(^{86}\) Gstrein (n 33) 125.

\(^{87}\) „Viele Lernanbieter haben ein zusätzliches, kostenpflichtiges Nachmittagsangebot. Die Befürchtung ist, dass Erkenntnisse aus dem schulischen Bereich generiert werden, die dann genutzt werden, um den Eltern etwas zu verkaufen. Im Sinne von ‘sie wollen doch das ihr Kind Abi macht, dann müssen sie aber auch diese Nachmittagsangebot nutzen’“. 
of a private learning platform adds to the discussion, ‘schools and data processor are struggling with providing it.’

Another issue raised by the participants, which shows that current legal requirements clash with common practices, is the requirement that parents and students must sign a consent form in order to allow the processing of student data by private parties. The participants made clear that the concept of informed and explicit consent, which assumes that the individual has free choice to agree or disagree, is not properly applicable in the school context. Since there are no equal ‘analogue’ alternatives to digital education, in practice students and parents would suffer from great disadvantages if they decided not to consent to the data processing (ibid). In particular, under the situation of pandemic related restrictions ‘a group pressure is created’ to accept the suggested digital tools. Even though the current conduct of informed consent is likely not to be upheld in front of courts, it is still used as schools are lacking an adequate alternative legal basis. Such an alternative could be the ‘public interest’ provision of Art 6 (1) lit e GDPR, which outlines that processing is lawful if ‘necessary for the performance of a task carried out in the public interest.’ However, to rely on this legal basis a specific law is required which outlines the purpose and conditions of the data processing for the respective public interest, and potentially includes individual remedies and safeguards against data abuse. Establishing such a new provision within the Education Acts of German states would be the best solution under the GDPR, argues one participant.

Nevertheless, establishing a novel legal framework without considering the necessity that educational institutions must be trusted and competent to protect students’ data falls short of solving the issue. Once enacted, such a legal basis would potentially undermine the ability of minors and parents to opt-out of data processing that takes place with tools of private players. One the one hand, a student representative considered the possibility to opt-out on an individual basis necessary, while pointing to ‘unsafe’ data infrastructure choices made by schools in the haste of the pandemic. On the other hand, if students and parents would be provided with better options for restricting the data collection according to their preferences, this would conflict with the public mandate of schools to provide education to all children and the smooth functioning of the school life. A participant argues that even though he considers ‘informational self-determination as very important, in some cases it clearly misses

88 „Transparenz ist ein Recht nach der DSGVO, aber die Schulen und Datenverarbeiter tun sich schwer diese herzustellen.“
89 „Es besteht ein Gruppendruck.“
the mark. We have compulsory education. (...) At the same time, however, we now have an excessive right to object to pedagogical [data] uses. This very quickly creates an absolute divergence.90

To summarize, the main conflicts surrounding the collection and use of student data are balancing the privacy and autonomy of minors with the benefits of monitoring and analysing the learning process, providing meaningful transparency despite limited resources, and finding an adequate legal framework for data processing.

5. Conclusion

In this chapter we investigated how the datafication of school with increasing dependence on data-intense infrastructure affects the privacy and autonomy of students. We argued that the situation of students in Germany is of particular relevance, as we analysed and discussed the datafication of schools in relation to privacy, data protection, as well as personal development. Despite the numerous requirements and safeguards envisioned by the European framework around the protection of personal data, it delivers no satisfactory results. As we show in section 3 formal guarantees such as the transparency principle, necessity to provide consent, a right to be forgotten, a right to not being solely dependent on automated-decisions and many others seem well intended. However, ultimately they do not seem to readjust the forces within the data economy and have little effect on the day-to-day data practices of schools. Additionally, we have looked at the concept of informational self-determination, which aims at protecting the personal space for development--an objective relevant in the context of datafied education. On the one hand, this right seems fascinating with its clear political mission, fostering democratic ideals and autonomy. On the other hand, much more consistent work and practice seem required to make it a reality and translate it into a governance framework and practice.

As we demonstrated based on a literature review and two case studies in pioneering schools throughout sections 4, many of the stakeholders are aware of the dilemmas and trade-offs the practice of the datafied school faces. It is also clear that the peculiarities of the German federated education system so far have hindered the development and implementation of an overarching vision. Yet, they also enabled the thriving of promising local initiatives. The learnings from these examples, however, demonstrate that engaging actively in sharing the digital infrastructure binds substantial resources, that most German schools likely are lacking. Regularly, consideration of the purpose and effect of datafication will hence remain only an after-thought.

90 „Die informationelle Selbstbestimmung ist enorm wichtig, aber teilweise schießt man mit diesem Rechtsanspruch deutlich über das Ziel hinaus. Wir haben eine Schulpflicht. (...) Gleichzeitig haben wir aber jetzt ein überbordendes Einspruchsrecht der pädagogischen Nutzung. Da entsteht sehr schnell eine absolute Divergenz“. 
At the end of this chapter, we must admit that more questions remain open than were answered, which is in itself a finding that should be considered. The engagement of all stakeholders in education will be necessary to develop a (more) common and inclusive vision of the datafied school that opposes invasive data logics commonly connected with Big Tech technology. It will be a key challenge for educational institutions to prove that they can be trusted with such sensitive data as produced over years in the learning context. Therefore, novel concepts such as ‘data trusts’ or ‘data stewards’ (Datentreuhand), which are envisioned as independent intermediaries overseeing the data flows and ensuring the rights of the individuals, might be promising in the domain of public education and help to relieve schools from the burden of securing data protection\(^\text{91}\). Finally, this chapter has also made clear that the traditional western ideals of education—such as free thought and expression—are under pressure. This has serious repercussions for democracies and free societies, which are dependent on humans that can develop and excel in unexpected ways.

\(^{91}\) The potential of a data trust for student data has been discussed in detail by Theresa Henne in earlier research. Please, contact the author for more information.
Literature


Andrejevic M and Selwyn N, ‘Facial Recognition Technology in Schools: Critical Questions and Concerns’ (2020) 45 Learning, Media and Technology 115


Beaulieu A and Leonelli S, Data and Society: A Critical Introduction (SAGE Publications Ltd 2022)


Broughan C and Prinsloo P, ‘(Re)Centring Students in Learning Analytics: In Conversation with Paulo Freire’ (2020) 45 Assessment & Evaluation in Higher Education 617


Füller C, ‘Schülerdaten - Das gläserne Klassenzimmer’ (Deutschlandfunk Kultur, 10 November 2020) <https://www.deutschlandfunkkultur.de/schuelerdaten-das-glaeserne-klassenzimmer-100.html> accessed 11 April 2022


Gstrein OJ and Beaulieu A, ‘How to Protect Privacy in a Datafied Society? A Presentation of Multiple Legal and Conceptual Approaches’ (2022) 35 Philosophy & Technology 3


Helbig M, Nikolai R and Wrase M, ‘Privatschulen und die soziale Frage Wirkung rechtlicher Vorgaben zum Sonderungsverbot in den Bundesländern’ (2017) 45 Leviathan 357


Jacquemain T, Der deliktische Schadensersatz im europäischen Datenschutzprivatrecht: unter besonderer Berücksichtigung der Schadensbemessung (1. Auflage, Nomos 2017)


Jones KML, ‘Advising the Whole Student: EAdvising Analytics and the Contextual Suppression of Advisor Values’ (2019) 24 Education and Information Technologies 437

Jones KML and McCoy C, ‘Reconsidering Data in Learning Analytics: Opportunities for Critical Research Using a Documentation Studies Framework’ (2019) 44 Learning, Media and Technology 52

Jones KML, Rubel A and LeClere E, ‘A Matter of Trust: Higher Education Institutions as Information Fiduciaries in an Age of Educational Data Mining and Learning Analytics’ (2020) 71 Journal of the Association for Information Science and Technology 1227


Lupton D and Williamson B, ‘The Datafied Child: The Dataveillance of Children and Implications for Their Rights’ (2017) 19 New Media & Society 780


OECD, ‘Were Schools Equipped to Teach – and Were Students Ready to Learn – Remotely?’ (2020) PISA in Fokus 108


‘Was ist eine Smart School?’ <https://www.smart-school.de/de/Smart-School> accessed 8 March 2022


Williamson B, ‘Calculating Children in the Dataveillance School: Personal and Learning Analytics’ in Emmeline Taylor and Tonya Rooney (eds), Surveillance futures: social and ethical implications of new technologies for children and young people (Routledge, Taylor & Francis Group 2017)


Zavala Barreda K, ‘Fuar de Alcance: Educación a Distancia En Zonas Rurales Peruanas Durante La Pandemia’ in Stefania Milan, Emiliano Treré and Silvia Masiero (eds), COVID-19 from the Margins (Institute of Network Cultures 2021)


Urteil vom 15 Dezember 1983, 1 BvR 209/83 (Bundesverfassungsgericht)

European Commission, 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 2021
Annex

Summary of Findings “Risks and Potential of Collection and Use of Student Data”

The table displays risks and potentials perceived by the participants of two Multi-Stakeholder Workshops and differentiates between internal data flows within the school and external data uses by third parties, such as edtech companies, public authorities or researchers.

<table>
<thead>
<tr>
<th>Potentials &amp; Uses</th>
<th>Risks &amp; Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal data use</strong></td>
<td><strong>Internal data use</strong></td>
</tr>
<tr>
<td>Better organisation and communication of daily school processes</td>
<td>Usability vs complexity of the IT-system</td>
</tr>
<tr>
<td>Support of teacher in capturing the student’s knowledge and skill level, which enables early detection of problems and better support</td>
<td>Sustainable data management</td>
</tr>
<tr>
<td>Better, more meaningful assessment formats</td>
<td>Data ‘overflow’, audience-targeted communication</td>
</tr>
<tr>
<td>Better understanding of students learning process and long-term development</td>
<td>Development of role-specific access rights</td>
</tr>
<tr>
<td>Individualized learning</td>
<td>Despite monitoring schools must remain a safe space to support students’ development holistically</td>
</tr>
<tr>
<td><strong>External data uses</strong></td>
<td><strong>Efficiency gains are used to reduce cost and personnel instead of improving quality of the education</strong></td>
</tr>
<tr>
<td>Research on the effectiveness of pedagogical concepts and the development of didactic models</td>
<td>Student data enables sensitive insights in students’ private life</td>
</tr>
<tr>
<td>Meta-monitoring and evidence-based education policymaking</td>
<td><strong>Both internal and external data use</strong></td>
</tr>
<tr>
<td>Improvement and innovation of learning platforms and tools</td>
<td>Lack of transparency on the collection, use and sharing of student data for students and parents</td>
</tr>
<tr>
<td></td>
<td>Students are discriminated against based on student data, student data creates stereotypes</td>
</tr>
<tr>
<td></td>
<td>Past data influences students’ future pathway, possibly creating path dependencies</td>
</tr>
<tr>
<td></td>
<td>Data disclosure because of cyber-attacks, vulnerability of IT systems and human mistake</td>
</tr>
<tr>
<td></td>
<td>Lack of understanding what data types are relevant to purposes of stakeholders</td>
</tr>
<tr>
<td><strong>External data use</strong></td>
<td><strong>Consistent procedure for data anonymisation and pseudonymisation</strong></td>
</tr>
<tr>
<td>Illegitimate access by third parties</td>
<td>General lack of transparency concerning data collection and use of private players</td>
</tr>
<tr>
<td>Students’ data becomes object of commercial interests</td>
<td>Deanonymisation</td>
</tr>
<tr>
<td>Student data is used to target parents and students with personalised advertisement</td>
<td>No systematic data collection across schools and regions</td>
</tr>
<tr>
<td></td>
<td>Consistent procedure for data anonymisation and pseudonymisation</td>
</tr>
</tbody>
</table>
### Description of the Workshop Participants

<table>
<thead>
<tr>
<th><strong>Multi-Stakeholder Workshop Dresden</strong></th>
<th><strong>Participants Multi-Stakeholder Workshop Berlin</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Learning facilitator</strong> at the USD, in direct contact with student analog or digital, active user of the USD’s system Edutech, hence deals with learning data, with attendance data etc</td>
<td><strong>IT project manager</strong> at FWU Institut für Film und Bild gGmbH, leads project on decentralized identity management at schools, therefore cooperates with providers of learning platform</td>
</tr>
<tr>
<td><strong>Research assistant</strong> at the Chair of Inclusive Education at the TU Dresden, responsible for the facilitation the communication between teachers and development team of the IT system, is interested in communication and learning data, sees quite some need for change in the technical infrastructure</td>
<td><strong>IT manager</strong> at bettermarks, adaptive learning platform, therefore, has contact with personal or pseudonymized data, as well as learning data that is usually anonymized for them</td>
</tr>
<tr>
<td><strong>Research assistant</strong> at the Chair of Inclusive Education at the TU Dresden, deals with student data, besides personnel data and learning data he is mainly concerned with surveys data</td>
<td><strong>Former data protection officer</strong> at bettermarks, adaptive learning platform, today coordinator for data protection inquiries</td>
</tr>
<tr>
<td><strong>Parent</strong> of two students at the USD, Professor at the TU-Dresden for information management, conducts research on group learning in the digital space in cooperation with international partners, therefore they collect for instance social interaction data to understand the dynamics between students and their learning development</td>
<td><strong>Project lead at non-profit</strong> Initiative D21 based in Berlin, which understand itself as network of digital society, connects economy, politics and civil society, interested in inclusive ) together, aim to shape digital change so that everyone benefits, it’s about participation, project lead of working group on Education &amp; Data Democracy, has written impulse paper on how AI could be applied in school context and as part of it worked also on risks and opportunities of student data</td>
</tr>
<tr>
<td><strong>Parent</strong> of a student at the USD, member of the parent council, user of Edutech and hence knows which data flows to/from the parents’ side</td>
<td><strong>Student and representative of Berlin Student Committee,</strong> committee has not worked on topics around student data or a data trust so far</td>
</tr>
<tr>
<td><strong>Student</strong> and <strong>Chair of the Saxony State Student Council</strong>, currently graduating from school (not the USD), student council has advocated for school experiments like the USD, so that data can be used and shared for research to bring momentum to society</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td></td>
</tr>
<tr>
<td><strong>Journalist</strong>, who focuses on education, in particular digital education, joins as ‘expert’ rather than as in his profession as a journalist</td>
<td></td>
</tr>
<tr>
<td><strong>Learning facilitator</strong> at the USD for primary school students, hence collects a lot of student data</td>
<td></td>
</tr>
<tr>
<td><strong>Sociology student</strong> at the TU-Dresden, researches on the topic of transparency in assessment situations in the digital school</td>
<td></td>
</tr>
</tbody>
</table>