Contents lists available at ScienceDirect

International Journal of Educational Development

journal homepage: www.elsevier.com/locate/ijedudev

Children's data protection in education: A case study of Google Workspace for Education in the European Economic Area

Elora Fernandes [*]

Centre for IT and IP Law - KU Leuven Centre for IT & IP Law (CiTiP) - IMEC, Belgium

ARTICLE INFO

Keywords:
Children's data protection
Educational technologies
Google Workspace for Education

ABSTRACT

Digital technologies are increasingly embedded in education, transforming not only the means of delivery, but also its values and purposes. The COVID-19 pandemic has caused a significant surge in the edtech industry, resulting in greater involvement of private entities in shaping the future of education and processing extensive volumes of children's data. Challenges related to protecting children's data in this realm have already been raised by several authorities across Europe. This paper analyzes cases related to Google Workspace for Education through a data colonialism lens, seeking to understand the strengths and limitations of public authorities' positions and whether the measures taken are adequate to address data protection issues associated with data colonialism. The findings suggest that an adequate enforcement of the General Data Protection Regulation is possible and powerful to protect children's data. However, this demands strong political and economic power to ensure compliance. It also falls short of addressing broader challenges posed by the prevailing business model, including familiarizing children with technologies that process data for predatory commercial purposes outside the school environment, as well as concerns regarding competition, public procurement, and data sovereignty.

1. Introduction

The education sector is often portrayed as being broken and stuck in the past (UNESCO, 2023b; Weller, 2020); as lagging other sectors in adopting technologies (Allen, 2022); as under digitized; and as "traditionally laggards when it comes to innovation" (Organization for Economic Cooperation and Development (Organization for Economic Cooperation and Development OECD, 2021, p. 3). This narrative frames the notion of development and improvement of education as inherently reliant on technology. Having the right tools would be, therefore, the way to solve the educational crisis, fueling a push for modernization and advancing technological solutionism.

Behind changes that should "only" be technical, however, "modernization" heralds a transformation of the school focused not only on the way it is organized but also on its values and purposes (Laval, 2019, p. 194). The implementation of digital technologies, especially the datafication of education, can actually not be fully understood without considering the context of early industrial capitalism and the historical demand for efficiency across various sectors of society (Barassi, 2020, p. 72). The measurement movement would not only refer to a new way of describing education, but also to a redefinition of education itself and its internal relationships (Lawn, 2013, p. 110). This shift ultimately aligns education with private-sector management practices and emphasizes economic efficiency.

With the intensification of neoliberal policies in the 1970s and 1980s, public education underwent alignment with private-sector practices and an intense marketization, either in the form of privatization or commercialization (Hogan and Thompson, 2021, p. 3). Private actors are ever more involved in a service that was once mainly provided by the state, resulting in an environment of "power-sharing, negotiation and competition, where decisions are made through a complex web of network interactions" (Castells, 2010, as cited in Hogan and Thompson, 2021, p. 3).

The COVID-19 pandemic has exacerbated this issue, leading to the swift adoption of fully remote online education as the preferred or ideal response to the resulting disruption (UNESCO, 2023a, p. 34). This triggered an abrupt growth of the educational technology (edtech) industry, further opening the door for private actors to shape the future of education and children's lives more than ever before. The urgency of decision-making often led to the implementation and, to this day, the continued use of edtech whose benefits lack scientific validation (Holmes, 2023; Kucirkova; Brod; Gaab, 2023) and, above all, pose risks

[*] Correspondence to: Sint-Michielsstraat 6 box 3443, Leuven 3000, Belgium.
E-mail address: elora.fernandes@kuleuven.be.

https://doi.org/10.1016/j.ijedudev.2025.103237
Received 2 October 2023; Received in revised form 3 February 2025; Accepted 14 February 2025
Available online 4 March 2025

to this group. A great part of these risks is associated with children's right to the protection of personal data, both as an end in itself and a means to protect other fundamental rights, such as privacy, non-discrimination, freedom of expression and protection against economic exploitation.

Data serve as a fundamental element that supports the advancement and utilization of these digital technologies (Tuomi et al., 2023, p. 12), especially those powered by artificial intelligence (AI). As children engage with them, data are continually processed not only to provide and improve the service, but also increasingly for commercial and surveillance purposes that are not always aligned with children's best interests.

Considering these challenges, public authorities worldwide—especially those responsible for enforcing data protection laws—are increasingly engaged with cases related to edtech and the risks these technologies pose to children. This paper aims to conduct a case study of one such technology, Google Workspace for Education, focusing on positions taken by these authorities within the European Economic Area (EEA). Google Workspace for Education was chosen not only for being one of the most widely used edtech solutions worldwide but also for Google's significant role in the digital ecosystem. In addition to pioneering the data-driven business model that dominates the online space today, Google's strong market position grants it seamless access to data collected through other edtech, as will be explored further.

Although being centered on the EEA, the challenges and conclusions outlined in this paper have clear global relevance, justifying its inclusion in this Special Issue. Given Google's monopolistic power and global reach, investigations and regulatory decisions concerning its technologies are frequently observed across various countries. Recent literature reinforces that data protection issues related to Google Workspace for Education are far from exclusive to Europe, as evidenced by studies in Brazil (Marrafon and Fernandes, 2020; Lima, 2020), Malaysia (Ya Shak et al., 2021), Egypt (UNESCO, 2023b) and the United States (Singer and Wakabayashi, 2020; Kimery, 2024). Therefore, the analysis presented in this paper, through the lens of positions taken by various EEA countries, identifies risk patterns that may emerge not only within the defined territorial scope but also on a global scale.

This becomes even more evident when considering that, over recent decades, the European Union (EU) has established itself as a global regulatory actor, particularly with regard to new technologies (Fahey, 2022). The EU influences other legal frameworks worldwide not only *de facto*—as regulated entities often standardize their global practices to simplify compliance—but also *de jure*—as many countries model their legislation on European frameworks, with the General Data Protection Regulation (GDPR) being a prime example (Bradford, 2020).

However, it is important to recognize that adaptations are always necessary. Universalist approaches risk ignoring the specificities of individual countries, particularly in terms of institutional design, socioeconomic conditions, and cultural contexts. Simply transplanting legislation can prove ineffective if robust enforcement mechanisms are not in place (Arora, 2019). After all, the existence of stringent legislation without adequate enforcement mechanisms can actually inadvertently legitimize harmful practices and hinder progress toward the realization of fundamental rights. This underscores the importance of examining the enforcement of data protection laws within the EU to identify potential legal and policy pathways for addressing these challenges.

Finally, it is important to note that the assessment in this paper will consider both the data protection concerns raised by the authorities based on GDPR requirements, and the lens of data colonialism. This approach highlights how even strict GDPR compliance may still fail to fully protect children's best interests and is particularly relevant when rethinking these issues in Global South contexts.

At a first glance, this might seem odd given Europe's role in historical colonialism. However, the EU is still quite technologically dependent on other countries such as the United States (US) and China, which exposes the specificities of data colonialism, due to the globalization and financialization of economy. This dependence and the need for digital sovereignty was one of the primary drivers behind initiatives such as the European Data Strategy and the adoption of more protective legislation, such as the Digital Services Act (DSA) and the Digital Markets Act (DMA). It also shows that data colonialism impacts all countries and populations, but certainly not uniformly, primarily due to the persisting social, economic, and cultural disparities rooted in historical colonialism.

In order to carry out this case study, therefore, the phenomenon of data colonialism is presented in Section 2. Section 3 discusses what is Google Workspace for Education and its main features, while Section 4 presents and assesses the identified positions taken by public authorities in EEA countries, with a focus on mapping the main actors and arguments employed to address the data protection concerns stemming from the use of this technology. Section 5 contextualizes the arguments put forth in these positions within the broader perspective of data colonialism, pinpointing key issues that relate to its four primary components, as well as digital sovereignty considerations. Finally, the last section provides a summary of the discussion and offers conclusive remarks.

2. Data colonialism

Data colonialism can be understood as the appropriation of human life through data (Couldry and Mejias, 2019, pp. xiii, xix). Unlike historical colonialism, data colonialism focuses not on natural resources and labor, but on human life and social relations through their conversion into data. Human life is referred to here not only in the present but also as the continuously expanding realm of exploitation. As our actions and innermost thoughts are increasingly taking place in the digital environment, there are apparently no restrictions on the extent to which human life can be exploited (Couldry and Mejias, 2019, p. 5).

The colonizing agents and the Empire itself built under data colonialism are also not the same as in historical colonialism. The *Cloud Empire* is a totalizing vision and a way of organizing businesses which drives data colonialism's expansion across social domains (Couldry and Mejias, 2019, xiii). It is implemented and extended by many players but primarily by the *social quantification sector*, the industry sector devoted to the development of the infrastructure required for the extraction of profit from human life through data (Couldry and Mejias, 2019, p. xiii). States, albeit less directly, also participate in these activities, either directly permitting or not regulating certain social relations. In-depth knowledge of the social world was once the prerogative of the state, but large technology companies now hold this privilege, with states becoming increasingly dependent on them.

Despite these main differences, historical colonialism and data colonialism share four key aspects, the first one being the *appropriation of resources*. Whereas historical colonialism was embedded in the *terra nullius* legal doctrine (according to which some lands belonged to no one), data colonialism treats data as a resource that is just there for the taking (Cohen, 2019, p. 48; Couldry and Mejias, 2019, p. 88). Data is appropriated based on a legal and social framing, turning life and social relations into a source of wealth, mirroring processes of accumulation by dispossession (Thatcher et al., 2016). Datafication is key for the process of commodification and privatization of data, with data is being produced not only with a main use in mind but also with the explicit purpose of market exchange.

The second component is the *unequal social and economic relations* that secure resource appropriation. Within historical colonialism this included moral or legal norms that would allow forced labor, for example. Within data colonialism, *data relations* are created between colonizing agents and citizens, which are asymmetrical due to the opacity of the transformation process that turn individual data points into big data (Thatcher et al., 2016). They provide corporations with a privileged overview of social relations which is incredibly powerful. Targeting vulnerable social groups is also a core strategy of data colonialism (Couldry and Mejias, 2019, pp. 67–68, 148–149). Although everyone's data contributes to data colonialism, certain individuals, such as children and particularly those at the bottom of the data pyramid (Arora, 2016) bear a higher cost.

The third component is the massively *unequal global distribution of the benefits of resource appropriation*. While historical colonialism would concentrate wealth in colonizing nations, data relations favors monopolization and the concentration of wealth in the hands of the colonizing agents (Couldry and Mejias, 2019). Finally, the fourth component is the spread of *ideologies that help make sense of the new order*. It was common within the historical colonialism framework to reframe "colonial appropriation as the release of 'natural' resources, the government of 'inferior' peoples, and the bringing of 'civilization' to the world" (Couldry and Mejias, 2019). Data colonialism is embedded in several ideologies, such as the ideology of connection, presenting as natural the connection of people and things (Couldry and Mejias, 2019, p. 16); the ideology of datafication, which perceives that all aspects of human life can and should be transformed into data; and the ideology of personalization, which could justify surveillance.

Regardless of the various ways and levels of granularity in which these ideologies can be described, what they have in common is the fact that they are all related to an overarching myth that

> technology, especially digital technology, is powerful, benign, and irresistible. There is no point whatsoever in opposing the Next Internet because the Cloud, Big Data, and the Internet of Things are too strong to overcome. Moreover, because it is a force for good, perhaps a major step along our evolutionary journey, it makes no sense to oppose them. The only reasonable choice is to yield to our digital future and embrace it enthusiastically (Mosco, 2017, p. 122).

This mainly occurs because of the asymmetrical extraction of value through datafication, which assumes that quantification and surveillance of all aspects of human life are natural and desired by all members of society (Thatcher et al., 2016, p. 991). This kind of myth empowers technologies and, especially, technology companies, while undermining human autonomy to determine their own path and destiny.

3. What is Google Workspace for Education?

Google Apps for Education was launched in October 2006 as an education-focused adaptation of Google Apps for Your Domain (Google, 2006). The beta version of Google Classroom became available in 2014 for selected schools (Magid, 2014), and in 2015 its mobile version debuted, together with the Google Classroom API, and a share button for websites (Perez, 2015). Google Apps for Education underwent a name change, becoming Google Suite for Education in September 2016 and later rebranded as Google Workspace for Education in 2020 (Google, 2020; Perez and Lardinois, 2016).

While not originally designed as a Learning Management System (LMS) (Lazare, 2021a), it constantly increased its features over time and teachers started to use it as a "hub" for educational content. Because of the COVID-19 pandemic, Google Classroom has increased from 40 million to 150 million users (Lazare, 2021b), making it one of the most used edtech worldwide.

Several editions of Google Workspace for Education are available to schools, with the Fundamentals one offered at no cost and premium editions requiring annual subscriptions (Google, 2023b, 2023a). With Google Workspace for Education Fundamentals, schools can access core[1] and additional[2] services, while Google Workspace for Education Standard includes premium security and IT features. The teaching and learning upgrade provides premium teaching and learning features to be added such as third-party add-ons, Microsoft Word support, call transcripts, YouTube Live Streams, among others. Finally, the Education Plus version includes all features in the Standard version and the Teaching and Learning Upgrade. Apart from the application suite, Google also offers Google Chromebooks, laptops designed to heavily rely on web applications using Google Chrome browser (Google, 2023c; Magid, 2014; Upson, 2011), as well as Smart whiteboards for using the Jamboard application (Google, 2023e).

Google Workspace for Education is structured to resemble in-person school processes. The central hub for activities within schools is Google Classroom where other applications can be embedded or linked. Within Google Classroom, educators can create and manage classes, assignments, and grades; give direct and real-time feedback; post announcements; engage with students in discussion fora; and schedule video meetings.

Google Classroom is also increasingly adopting AI-driven tools. One notable application is the introduction of "Practice Sets", which leverages AI to transform teaching content into interactive assignments for personalized learning. Educators can either create their own questions or choose from a database, with AI suggesting specific skills that would be emphasized in that activity (such as solving equations or writing thesis statements). Teachers select the most appropriate option and students receive hints if they face any challenge in solving it. This can also be implemented in YouTube videos.

Students get real-time feedback "[a]nd when they get an answer correct, practice sets will celebrate their success with fun animations and confetti" (Kiecza, 2022). The application also includes an autograding tool, as well highlights on the students' performance, enabling educators to identify areas where students may need further support. Personalized learning is also implemented by the add-on read-along, which provides real-time feedback to children learning how to read (Sinha, 2023).

Classroom analytics provide educators with insights into assignment completion rates, grade trends, and Classroom adoption, with the possibility to delve into the individual student level to better provide support (Sinha, 2024). Additionally, generative AI is increasingly being integrated into Google Workspace for Education. For example, Duet AI is

[1] The list of core services include: Client-Side Encryption, Cloud Identity Services, Duet AI for Google Workspace, Enterprise Data Regions, Gmail, Google Calendar, Google Chat, Google Cloud Search, Google Contacts, Google Docs, Google Sheets, Google Slides, Google Forms, Google Drive, Google Groups for Business, Google Jamboard, Google Keep, Google Meet, Google SIP Link, Google Sites, Google Tasks, Google Vault, Google Voice, Google Workspace Assured Controls, Google Workspace Migrate, Meet Global Dialing, Workspace Additional Storage, and Workspace Add-Ons (Google, 2023d).

[2] The list of additional services include: Applied Digital Skills, Assignments, Blogger, Brand Accounts, Campaign Manager 360, Chrome Canvas, Chrome Cursive, Chrome Remote Desktop, Chrome Web Store, Classroom, CS First, Early Access Apps, Experimetnal Apps, FeedBurner, Google Ad Manager, Google Ads, Google AdSense, Google Alerts, Google Analytics, Google Arts & Culture, Google Bookmarks, Google Books, Google Business Profile, Google Chrome Sync, Google Cloud, Google Colab, Google Developer, Google Domains, Google Earth, Google Fi, Google Groups, Google Maps, Google Messages, Google My Maps, Google News, Google Pay, Google Photos, Google Play, Google Play Console, Google Public Data Explorer, Google Read Along, Google Search Console, Google Takeout, Google Translate, Google Trips, Location history, Looker Studio, Managed Google Play, Material Gallery, Merchant Center, Partner Dash, Pinpoint, Play Books Partner Center, Programmable Search Engine, QuestionHub, Scholar Profiles, Search Ads 360, Search and Assistant, Socratic, Studio, Third-party App Backups, Tour Creator, and YouTube (Google, 2023d).

designed to assist teachers across the suite's applications, aiding them in drafting lesson plans in Google Docs, generating images in Google Slides, or building spreadsheets in Google Sheets.

Even with the use of digital technologies, the educational processes enabled by Google Classroom largely continue to reproduce a hierarchical classroom structure and a behaviorist approach to learning (Gleason and Heath, 2021). Within the pedagogical domain, the mechanisms and structures of formal schooling are abstracted to fit a predefined template for participation. As Perrotta et al. (2021, p. 107) explain this is encapsulated in the notion of a "doubly articulated pedagogy", which encompasses three main components:

> a) the role of Google, the platform proprietor, in establishing the strategic outlook and the 'rules of the game'; b) the various forms of integration enabled by a proprietary API, which simultaneously brackets and extends pedagogy; and c) the multiple divisions of labour which are enabled by the platform dynamics, and upon which the platform as a whole depends.

While Google asserts that teachers should play a more significant role than technology (Langreo, 2023), these components mean that important decisions regarding the platform's design and functionality are delegated to developers, positioning Google as an arbiter in the educational environment (Vaidhyanathan, 2011). This is not the result of a democratic and inclusive decision, but is rather imposed by the infrastructure itself (Perrotta et al., 2021, p. 108).

3.1. *The role of Google Workspace for Education in Google's business model*

Data is perceived as a valuable resource to be exploited and commodified for market exchange. This notion is deeply entrenched in today's predominant data-driven business models, primarily centered around targeted advertising. Notably, Google has played a significant role in implementing and perpetuating this practice within the digital economy. Having discovered how data related to search queries (behavioral surplus) could be used to increase the profitability of advertisement, Google revealed new possibilities of inferring and deducing people's thoughts, intentions and behaviors. This was created as a one-way mirror based on asymmetries of knowledge and power (Zuboff, 2019).

In order to scale and gather more data, so predictions were more "accurate", there was a need not only to attract more users, but to be ever more present in users' lives through different means. Google started to expand to other areas beyond search such as providing services for schools, what would also help them reach younger audiences.

One of the characteristics that make Google Workspace for Education attractive is the provision of its services free of charge or for an affordable fee. An interesting finding in the Dutch case that will be discussed below was that, apart from the possibility to store specific consent data within the EU and the provision of additional security management options, there were no other significant distinction in data protection between the free and paid versions of Google Workspace for Education (Nas and Terra, 2021a, p. 5), showing how the business model focused on harnessing data is present in both options.

Although there may be no to little monetary exchange between the end user and digital platforms, the former has to give up something to sustain the market, be it data, attention, time or another form of currency. Big tech companies retain users through design practices that can be manipulative or deceptive, leading them to spend excessive time in digital environments or prompting them to repeatedly return to the platform (Danish government's expert group on big tech, 2023). Therefore, what is mistakenly understood as "for free" or relatively cheap may be explored in the expense of individual and collective externalities that should also be factored in (Trzaskowski, 2022, p. 234), including concerns related to competition, data protection, and, more broadly, children's best interests.

One of the main arguments Google uses to promote its products within schools is that it does not display advertisement in the core services of Google Workspace for Education, nor does it collect user's data for this purpose. Therefore, it is important to delve deeper to better understand what could be Google's economic incentives to invest in this field.

After analyzing the institutional logic behind the involvement of transnational technology corporations in education, Patil (2023) reached the conclusion that financial gain was their main drive. This could take the form of brand recognition, market development or workforce development, all of which can be seen in Google Workspace for Education.

First, Google's marketing strategy heavily relies on brand loyalty. The focus is not necessarily on immediate transactions, but on profitable growth in the long term. The so-called costumer lifetime value (CLV) is often used as a metric to measure the total value a business receives from a single customer over their entire relationship, and is seen as "an ideal way to acquire, develop, and retain the most valuable customers for business growth" (Fader and Hoyne, 2021, n.p.). Early exposure to the products creates familiarity, encouraging life-long learning and building community experiences.

It also encompasses expanding their business to increasingly more areas. In the case of Google, the focus of their products go from search to education, shopping, patents, finance, communication, productivity, maps, healthcare, and operational systems. Veliz (2022) contends that these are not necessarily products designed for people, but rather new ways to collect more and different data from them.

A second important aspect to consider is that Google Workspace for Education encompasses two different kinds of services (core and additional services), as described above. Additional Services "are designed for consumer users and can optionally be used with Google Workspace for Education accounts if allowed for educational purposes by a school's domain administrator" (Google, 2023d, n.p.). This differentiation is crucial, as it determines how students' and educators' data will be processed by Google.

While within core services no advertisements are shown and no personal data are processed for this purpose, additional services may do so. Personal data could also "be used to provide, maintain, protect and improve additional services, and to develop new ones" (Google, 2023d, n.p.). In this sense, if the educator uses one of the additional services within the classroom, personal data could be processed under less strict policies and advertisements can be shown to students.[3]

Google also encourages parents and guardians to create a second account for the child, which can be linked to the school account through the Family Link, as this would "empower" them to set parental controls across accounts (Hooper et al., 2022). However, what does not necessarily remain clear is that this action might inadvertently prevent the child from benefiting from the protective measures instituted by the school within the school account.

Therefore, the data-focused business model persists, and the core services may be serving as a bait to acquire more users and as a pathway for children to move from privacy-friendly environments to data-harvesting ones (Hooper et al., 2022, p. 55). The seamless user interface blurs the distinctions between core and additional services, resulting in users easily transitioning between them without being aware of the differences in terms of data protection and the associated consequences (Hooper et al., 2022, p. 55).

A third important aspect is that to support Google's commercial interests, data do not need to be processed only for targeted advertising.

[3] It is important to mention that Article 28(2), of the Digital Services Act (DSA), has prohibited providers of online platforms to present advertisements on their interface based on profiling using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor.

Google can use data to refine and enhance their products and services. This involves analyzing user data to gain insights into consumer behavior, preferences, and trends. By understanding how users interact with their applications, Google can improve design, develop new features, and tailor its services to better meet the needs and desires of its (future) customers. Additionally, data can be used for improving and training Google's AI tools. In this sense, children's data become valuable to understand preferences within a specific generation, family dynamics, future trends, etc.

A fourth aspect is that Google can access children's data indirectly, through other edtech. In a study about 163 edtech products, Human Rights Watch discovered that 80 % were found with at least one embedded Google software development kit (SDK). The NGO also found that edtech companies would in some instances send or grant access to children's data to Google's advertising division (Human Rights Watch, 2022). Its "vertically integrated chain of platforms and algorithms" (Couldry and Dijck, 2015, p. 4) facilitates this process, as Google currently dominates the advertising technology (adtech) market both in terms of selling advertising space on its own websites and apps and being an intermediary between advertisers and publishers that can supply add space.

Fifth, the integration and interoperability of Google Workspace for Education with other applications through the Google Classroom API is also fundamental for expanding Google's business model. With the API, Google can attract developers and software providers, outsourcing the task of expanding the platform's functionalities in order to "'enrich' the classroom experience, as long as they remain aligned with the overarching data ontology" (Perrotta et al., 2021, p. 103).

Interoperability is also important for maintaining Google's relevance, increasing its adoption and customer retention. The amount of data that it has access to also increases. The use of the API "allows Google to monitor and regulate how data are being exchanged, and how functionalities and their associated practices are integrated in the Classroom experience" (Perrotta et al., 2021, p. 103). This gives Google a powerful role of gatekeeper for the edtech industry, setting the rules for third party providers to integrate with Google Classroom and share data between them (Williamson, 2021).

Finally, the provision of Google Classroom as a free and accessible edtech strategically aligns with Google's narrative of social responsibility. This builds a positive brand image and positions the company as an entity that cares for positive societal impact (Magalhães and Couldry, 2021).

4. Positions from public authorities regarding Google Workspace for Education in the EEA

In recent years, European authorities have been actively assessing Google Workspace for Education's operations and their impact on children's privacy and data protection. The auditing capabilities of public authorities, especially Data Protection Authorities (DPAs),[4] and the publication of Data Protection Impact Assessments (DPIAs)[5] in certain cases, allowed an in-depth analysis of the features of Google Workspace for Education. This level of scrutiny would be unattainable solely through the information publicly disclosed by the company, such as in Terms of Service (ToS) and Privacy Policies.[6]

In order to identify positions related to data protection concerns regarding the use of Google Workspace for Education in the EEA—which in this paper broadly encompass any stance taken by public authorities related to Google Workspace for Education, such as binding decisions, advice, guidelines etc.—two main methods were employed.

First, I searched the databases of DPAs that are part of the European Data Protection Board (EDPB). This includes not only the DPAs in each of the EU Member States (and, in the case of Germany, in each of its *Länder*), but also those in the three countries that are part of the EEA: Iceland, Liechtenstein, and Norway. This search was supplemented by cross-referencing with the GDPR Hub (2024) and GDPR Enforcement Tracker (2024) websites.

Second, the literature reviewed also unveiled significant positions regarding the use of the technology in certain countries and regions that were not covered in the initial search, such as the decision taken by the French Minister of National Education and Youth and the position of the Flemish Supervisory Commission for the processing of personal data[7] in Belgium. Ultimately, positions regarding the use of this technology by schools were located in Belgium, Denmark, Finland, France, Germany, Iceland, Netherlands, Norway, Spain, and Sweden as of June 2024.

This section undertakes an analysis of these positions, aiming to understand the systematic functioning of Google Workspace for Education and the risks it can pose to children's privacy and data protection. The table below briefly describes the main aspects of each position, while Section 4.1 onwards aim to find convergences, divergences, and gaps, focusing on the concerns raised by the authorities that are related to GDPR requirements.

Country	Authority	Main aspects of the position
Belgium	*Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens* (VTC - Flemish Supervisory Commission for the processing of personal data)	In June 2023, the VTC published a non-binding position on the use of Google Workspace for Education by primary and secondary schools in the Flemish region. It also referred to previous guidelines on the procurement of software services and suppliers by public authorities in the Flemish region (see VTC, 2021, 2023a, 2023b). *Main aspects discussed in the position:* • The relationship between Google and schools reflects a power imbalance, with Google holding greater

(*continued on next page*)

[4] According to Article 58, GDPR, DPAs are vested with several investigative powers, including the ability to carry out data protection audits. This means they can systematically and independently assess whether an organization complies with the GDPR, without being limited to the organization's claims or the content of its policies and technical documentation.

[5] A DPIA is a procedure that helps controllers identify and mitigate risks within data processing activities. A DPIA must be performed when the processing is likely to result in a high risk to individuals. While Articles 35 and 36 of the GDPR establish the main rules regarding DPIAs, DPAs are required to publish a list of specific situations where they must be carried out (Article 35 (4), GDPR).

[6] This is especially important considering that what is stated in the ToS is not necessarily true. A recent leak of Google's internal files, for instance, revealed that the company processes data in ways not disclosed in their public policies (Sato, 2024).

[7] Due to the existence of other DPAs in the country, the role of the VTC was brought up in a parliamentary question (La Chambre des Représentants, 2023). It discussed a possible cooperation agreement between the Belgian DPA and the VTC due to different interpretations given to the GDPR, which could create legal uncertainty. The government responded by indicating that discussions are still ongoing regarding the powers of the VTC and its relationship with the Belgian DPA. However, it highlights that the Belgian DPA is the sole supervisory authority under the GDPR within the country. Although the GDPR does not exclude the existence of more than one supervisory authority in the same MS, the VTC would only be able to act as one if it fulfils the conditions set out in Chapter 4 of the regulation (see also decision 26/2023 of 16 February 2023, of the Belgium Constitutional Court (Grondwettelijk Hof, 2023)). The VTC is, therefore, only focused on the public authorities of the Flemish region and is in charge of providing them with advice on the matter of data protection.

(*continued*)

Country	Authority	Main aspects of the position
		influence over educational practices and data; • Ambiguities exist regarding the roles and responsibilities of Google and schools within the GDPR; • The requirement for schools to carry out DPIAs may be challenging and impractical in practice.
Denmark	*Datatilsynet* (Danish Data Protection Authority)	In September 2021, the Danish DPA issued a decision regarding the use of Google Workspace for Education by the Helsingør municipality after receiving complaints from parents and a data breach notification from the municipality. The case was reassessed in July and August 2022, but the ban was upheld. Following meetings with the KL (Local Government Denmark), representing the 98 Danish municipalities, and the Danish Agency for IT and Learning, the ban was lifted in September 2022, but an order for compliance was issued (see Datatilsynet - Danish Data Protection Authority, 2021; Datatilsynet - Danish Data Protection Authority, 2022a, 2022b, 2022c, 2022d, 2022e, 2022f). In June 2023, the KL provided a response to the DPA, which issued its fifth decision in January 2024 (Datatilsynet - Danish Data Protection Authority, 2024). The decision affected 98 municipalities in Denmark. *Main aspects discussed in the decisions:* • Lawful bases for processing data within Google Workspace for Education by schools; • Data minimization; • Lack of documentation kept by the controller; • Lack of risk assessment of the security of processing and of a DPIA.
Finland	*Tietosuojavaltuutettu* (Finish Data Protection Ombudsman)	In April 2018, the Finish DPA initiated an investigation related to the use of Google Suite for Education by a Finish school. The controller was reprimanded and ordered to bring processing operations into compliance (Tietosuojavaltuutettu, 2021). *Main aspects discussed in the decision:* • Lawful bases for processing data within Google Workspace for Education by schools; • Risks arising from accepting Google's ToS; • Lawfulness of data transfers.
France	*Ministère de l'Éducation Nationale et de la Jeunesse* (French Minister of National Education and Youth)	In August 2022, a member of the French National Assembly, Mr. Philippe Latombe, raised concerns with the French Minister of National Education and Youth regarding the use of Microsoft Office 365 in schools, mentioning risks to competition and data sovereignty. In his written response, the French Minister stated that free service offers would, in principle, be excluded from the scope of public procurement. He also indicated that Microsoft Office 365 would not comply with the Cloud at the Centre Doctrine. This decision was extended to Google Workspace for Education, and French educational institutions were demanded to use alternative tools (see Assemblée Nationale, 2022a, Assemblée Nationale, 2022b, p. 3866; Borne, 2023; Dinum, n.d.).
Germany	*Hessischer Beauftragter für Datenschutz und Informationsfreiheit* (Hesse DPA); *Oberverwaltungsgericht für das Land Nordrhein-Westfalen* (Higher Administrative Court of North Rhine-Westphalia)	In August 2018, Microsoft announced the end of its collaboration with Deutsche Telekom in providing Microsoft cloud services, including Office365, under strict German jurisdiction (the so-called German Cloud). After this change and having received several complaints from teachers and school administrators, German Land of Hesse's DPA prohibited the use of Microsoft Office 365 in schools since children's data were being stored in a European Cloud in July 2019. The same decision was also extended to Google and Apple services using a similar cloud. A month later the ban was lifted by the DPA, which decided to "temporarily tolerate" the use of the tool under certain conditions and subject to further examination (Dedezade, 2018; Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 2019a, 2019b; Poortvliet, 2018). *Main aspects discussed in the decision:* • Lawfulness of data transfers; • Digital sovereignty; • Lawfulness of the collection of telemetry data. The use of Google Services was also prohibited at one of Dortmund's seven secondary schools, after a student raised privacy concerns, leding to his refusal to use the platform in 2021. Despite the school offering an alternative solution, it was rejected as it was believed that

(*continued on next column*)

(*continued on next page*)

(*continued*)

Country	Authority	Main aspects of the position
		participating in school activities without discrimination was not possible. The student filed a complaint with the Petitions Committee of the State Parliament and, after appeals, the case reached the Higher Administrative Court of North Rhine-Westphalia. The school was found to be unable to prove the use of the platform in compliance with the GDPR, and the case was closed following an agreement between the parties to discontinue its use (mrtee, 2023a, 2023b).
Iceland	*Persónuvernd* (Icelandic DPA)	The Icelandic DPA initiated an *ex-officio* investigation, including audits, within the scope of the EDPB's broader initiative on assessing the use of cloud services by public authorities. It assessed the processing activities of five municipalities that used Google Workspace for Education in primary schools (see Persónuvernd, 2023a, 2023b, 2023d, 2023c, 2023e). *Main aspects discussed in the decisions:* • The municipalities did not ensure that data were processed only for the previously-agreed purposes; • The municipalities did not assess the compatibility of further processing by Google in relation to service data; • The DPIA does not meet minimum requirements of Article 35, GDPR; • The municipalities did not implement additional protection measures for data transfers based on Standard Contractual Clauses (SCC).
Netherlands	*Autoriteit Persoonsgegevens* (Dutch Data Protection Authority)	In February 2021, SURF—the collaborative organization for IT in Dutch education and research—and SIVON—a cooperative of school boards in primary and secondary education—disclosed that a DPIA of Google Workspace for Education had been commissioned by the University of Groningen and Amsterdam University of Applied Sciences. Completed on 15 July 2020, the DPIA identified ten high[1] and three low[2] data protection risks affecting data subjects when they used Google Workspace for Education. After Google had mitigated some of the risks, SURF and SIVON asked advice from the Dutch DPA, who suggested to discontinue the use of Google Workspace for Education before all issues were solved. In July 2021, Google and the educational institutions reached an agreement to sufficiently mitigate all identified risks. A new DPIA was requested, which identified new risks. In December 2022, SIVON and SURF reported Google's progress in addressing the risks identified in the 2021 DPIA, with ongoing efforts to solve remaining issues by mid-June 2023. Despite negotiations, the DPA was still concerned about the Minister's additional findings, especially if any substantial privacy risks for students remained. On 20 April 2023, the Ministry of Education, Culture, and Science informed the House of Representatives how the advice from the DPA was followed. A verification report was issued by Privacy Company confirming the measures implemented by Google. However, the new assessment revealed new potential risks, which were meant to be discussed separately between SURF, SIVON, and Google. Additionally, a separate process started in the beginning of 2023 to address concerns pertaining to data transfers, particularly to the USA. A Data Transfer Impact Assessment (DTIA) was underway and was anticipated to conclude in autumn 2023 (see AP, 2021; Ministerie Van Onderwijs, 2023; Nas, 2021; Nas and Terra, 2021b, 2021a; Nas and Terra, 2023; Privacy Company, 2021a, 2021b; SURF, n.d.-b; SURF, n.d.-a; SURF, 2021a; SURF, 2021b; SURF, 2023a; SURF, 2023b; SURF, 2023c; SURF and SIVON, 2023; Terra et al., 2023).
Norway	*Datatilsynet* (Norwegian Data Protection Authority)	In Norway, several municipalities have adopted Google Workspace for Education in primary and lower secondary schools. Based on parents' complaints, the DPA has taken a closer look at three of them. Although based on different complaints and different grounds, the three decisions focused on the same four issues identified by the authority. *Main aspects discussed in the decisions:* • The municipalities have not kept a log of processing activities taking place on

(*continued on next column*)

(*continued*)

(*continued on next page*)

(*continued*)

Country	Authority	Main aspects of the position
		students' Chromebooks and in G Suite for Education; • They have not implemented appropriate technical and organizational measures to achieve a level of security appropriate to the risk; • They have not conducted a privacy impact assessment of the use of Chromebooks and G Suite for Education in schools; and • They have not provided adequate information to enable students and parents to safeguard their interests and privacy when using Chromebook and G Suite for Education (Datatilsynet - Norwegian Data Protection Authority, 2020a, 2020b, 2020c, 2020e). After dealing with these three cases, the DPA issued guidelines applicable to all municipalities within Norway that used Google Chromebooks and Google Workspace for Education (Datatilsynet - Norwegian Data Protection Authority, 2020d).
Spain	*Agencia Española de Protección de Datos* (AEPD – Spanish Data Protection Agency),	In the case of Spain, two decisions are important for the scope of this paper. The first one originated from a complaint of a parent, dated July 2021, who argued that they were not consulted for the implementation of G Suite for Education in a school under the organization of the *Consejería de Educación, Universidades, Cultura y Deportes del Gobierno de Canarias*. The second one is related to the use of Google Workspace for Education at Colegio Menor Nuestra Señora de Loreto. It also originated from a parent's complaint dated August 2021, who argued that consent had not been provided for the use of the tool within the school (see AEPD, 2023a, 2023b, 2023c). *Main aspects discussed in the decisions:* • Lawful bases for processing data within Google Workspace for Education; • Lack of proper information provided to data subjects; • Lack of clarity related to roles and responsibilities of controllers and processors; • Incompleteness of DPIA.
Sweden	*Integritetsskyddsmyndigheten* (IMY - Swedish Authority for Privacy Protection)	A procedure has been initiated by the Swedish authority to investigate the *barn- och utbildningsnämnden* (Children and Education Board), in Östersund Municipality, in relation to the introduction of Google Workspace for Education in 24 schools in the fall of 2020. After failed attempts to reach compliance, the IMY imposed an administrative fine of SEK 300,000 (approximately 26 thousand euros) against the board (see IMY, 2023a, 2023b). *Main aspects discussed in the decision:* • Lack of documentation kept by the controller; • Lack of risk assessment of the security of processing and of a DPIA; • Lack of appropriate safeguards to mitigate identified risks.

(*continued on next column*)

(*continued*)

[1]The ten high data protection risks identified by Privacy Company were: Lack of purpose limitation (in relation to customer data); lack of purpose limitation (in relation to diagnostic data); lack of transparency (in relation to customer data); lack of transparency (in relation to diagnostic data); lack of lawful grounds for processing personal data; missing privacy controls; privacy-unfriendly default settings; the use of multiple Google accounts; lack of control of subprocessors; lack of access by data subjects to their personal data.

[2]The three low data protection risks identified by Privacy Company were: Unlawful access to customer data and diagnostic data in the USA by the cloud provider; the chilling effect generated by the employee monitoring system; and the impossibility of deleting individual diagnostic data.

4.1. Roles and responsibilities

An important topic that stands out in almost all positions is the difficulty in delimiting the roles and responsibilities[8] of schools and Google regarding the processing of personal data. This discussion was pivotal within the Dutch case and the contracts analyzed by Privacy Company. In that situation, Google qualified itself

> as [a] data processor for the personal data in Customer Data it processes through the Core Services in G Suite (Enterprise) for Education (described as the Customer Data in this DPIA) [and] as data controller for the Google Account, most of the Additional Services including Chrome OS and the Chrome Browser, the Diagnostic Data and other services related services such as Feedback (Nas and Terra, 2021a, p. 6).

For other services, the roles were considered not to be clearly defined or were unlawfully designated, as Google could not be considered neither a sole controller nor a processor for some activities. Google was able to process some personal data solely because of its relationship with the educational institutions, which, according to the EDPB guidelines (EDPB, 2021), would demand joint controllership. The joint controllership was, however, not a possibility in cases where the purposes of the data processing were not aligned with the legal duties of the school to provide education, something also identified by the Danish DPA. The only situations where this would not apply would be when Google

[8] Within the GDPR, "'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law", while "'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (Article 4(7)-(8)). Defining the correct role within the GDPR is crucial for determining the actor's responsibility.

processes data for its own legitimate business purposes, like invoicing, or when they are required to disclose data to authorities (in cases where Google is not allowed to forward this request to schools) (Nas and Terra, 2021a, p. 107).

A similar situation was identified in Iceland, where the municipalities under investigation did not ensure that data were only processed for the purposes they established as controllers and under their instructions. Google processed "service data" independently and for its own purposes, without any previous agreement with the municipalities.

Apart from identifying ambiguities regarding who determined the means and purposes of data processing, the VTC in Belgiumn found it unrealistic to consider schools as controllers in some cases. The power imbalance between schools and Google made it difficult for the former to discern which data are being collected for each purpose, thereby posing a challenge for them to monitor Google's activities as a data processor.

In some instances, the lack of properly defined roles and responsibilities was also attributed to the acceptance of the standard ToS. The AEPD found that the ToS lacked precision regarding the roles and responsibilities for each processing activity under Article 28, GDPR, and should have been supplemented by another document specifying them.

In the Finnish case, the DPA found that by accepting Google's ToS as it was, the controller undermined its ability to adequately control and supervise the processing of personal data, a concern also recognized in a previous DPIA. Similarly, in the Danish case, the Helsingør municipality was unaware of many changes made by Google to its ToS, which contributed to a breach of students' data. Lastly, the VTC in the Belgian case also highlighted that the purposes and means of processing personal data could change at any time when Google modifies its ToS, posing a concern for schools as controllers.

The common thread connecting the issues described above is the factual influence exerted by Google on the purposes and means of the processing activities. As controllers in the majority of cases, schools bear the responsibility to ensure that the processor adheres to data protection laws and implements necessary safeguards. Especially when it comes to the adoption of AI systems, schools must understand their functioning and the decision-making processes involved, as they must explain this information to data subjects.

In this sense, a specific analysis of each data processing activity or set of processing activities must take place. While it may be evident that schools act as controllers and Google as the processor in tasks such as registering students and staff on the platform, it is not so clear when the platform processes data to offer personalized learning activities within Google Classroom, for instance.

Even when schools can agree with the purposes for processing personal data, it is still necessary to check whether Google is actually deciding *essential means* of the processing activities, such as which data are processed and for how long, if decisions are automated, etc. Due to schools' frequently limited expertise and resources in understanding the operations of AI systems, especially when trade secrets are involved, and the lack of explicit prior instructions provided to Google (depending on how the ToS have been signed and the influence exerted by the schools on its terms), a scenario where Google should be considered a joint controller in these cases is highly likely.

4.2. Purposes for processing personal data

Defining the purposes for which personal data are processed is a crucial step towards compliance with the GDPR. Transparency regarding these purposes is essential to adhere to principles such as purpose limitation, data minimization, and lawfulness, as well as for data subjects to exercise their rights. The cases analyzed for this paper show that the purposes for which student data were processed were not explicitly defined and detailed enough to determine what kind of processing of personal data is encompassed by them.

The separation of core services from additional services, along with the distinction between customer data and service data, create layers of complexity and pose practical challenges. A first issue would be the lack of a full list of types of data collected within each of these categories. This would be essential for the specification of the purposes and is all the more important when children's data and sensitive data are processed. The second issue is the lack of a proper list of the purposes for which data are processed.

In the cases of Germany and the Netherlands, particular attention was drawn to the irregular processing of telemetry and diagnostic data. Telemetry data is collected through a process that involves the automatic collection, transmission, and measurement of data from remote sources using sensors and other devices. These data are only pseudonymized, meaning that it was still possible to identify individuals under certain circumstances. Diagnostic data, often collected via telemetry, provides valuable insights into the devices in use and the performance of the applications deployed (Hessel, 2022).

At the time of the first DPIA carried out by Privacy Company within the Dutch case, Google had not made available any public documentation regarding the specific purposes for which it processes diagnostic data, whether to be used in core or additional services. Information about all the purposes for which Google processed data was also not clearly and thoroughly available, especially when Google was acting as a data processor (Nas and Terra, 2021a). Although the narrative behind the use of diagnostic data is often linked to the implementation of security measures on the platform, the lack of clear purposes means that one cannot be sure of their beneficial use.

Within the Icelandic case, the DPA stated that when municipalities decide to deploy cloud services in primary schools, they are responsible for ensuring that students' data are not further processed for incompatible purposes, such as when data were used to refine Google services and introduce new functionalities.

When it comes to the separation of core and additional services within the Dutch case, even when schools were mandated to disable the latter—since they do not control the data processing and Google lacks a legal basis to process such data—students often circumvented this by creating personal accounts, facilitating smoother integration between services. In order to avoid spill-over of data, schools would also need to technically prohibit simultaneously signing-in with two or more Google accounts in the same device (Nas and Terra, 2021b, p. 11). The DPIAs also highlighted that data flow between accounts and among core and additional services lacked clarity. Consequently, even when the school initially defines the purposes for processing student data, the structure of the services facilitates the collection of data for commercial purposes.

Although schools could technically restrict access to these services within its premises, as well as the simultaneous log-in, they would not be able to prevent students from creating a personal account (Nas and Terra, 2021b). As this is often essential or convenient in some situations, such as for avoiding persisting consent banners, and accessing YouTube, Google Photos, Google Maps etc., it is unavoidably done by students or their parents. Children become accustomed to the technology used in the classroom and to the additional services, given the natural integration between them. Therefore, the creation of personal accounts will often occur either during their time in school, for using the additional services, or later for accessing materials they would like to keep, for instance.[9] Schools have, thus, an important role in introducing certain technologies

[9] In the USA, for example, some schools were even directly encouraging graduating students to convert their Google Workspace for Education accounts into personal accounts: "Every year, several million American students graduate from high school. And not only does Google make it easy for those who have school Google accounts to upload their trove of school Gmail, Docs and other files to regular Google consumer accounts — but schools encourage them to do so. This month, for instance, Chatfield Senior High School in Littleton, Colo., sent out a notice urging seniors to 'make sure' they convert their school account 'to a personal Gmail account'" (Singer, 2017).

and transforming children into consumers for other products.

In a study conducted on the ToS and privacy policies adopted by Google Workspace for Education in 2021, the same ones analyzed by Privacy Company, Hopper et al. (2022) also demonstrated the challenges in identifying the data collected by Google and the purposes for which they were processed, as it employs various terms to describe data types, leading to confusion and complexity.

Lastly it is important to highlight that in all cases there was minimal to no discussion regarding the use of AI systems within Google Workspace for Education and their impact on the purposes of personal data processing. If data collected to provide services to schools is also being used to train AI or improve Google's services, a careful analysis under Article 6(4) of the GDPR would be imperative, as well as other relevant provisions such as Article 22.

4.3. Lawful bases

The appropriate legal basis for processing data within Google Workspace for Education by schools was widely discussed by the authorities. Some cases were brought to their attention due to complaints regarding the absence of parental consent for schools to process data on the platform. The Danish DPA clarified that the Municipality's use of Article 6(1)(e), i.e., the processing of data based on a task carried out in the public interest, was appropriate, and consent was not applicable for the provision of Google Workspace for Education Core Services and the creation of individual user accounts within the platform.

In Norway, some municipalities relied on consent, the performance of a contract, and a legal obligation to process students' data. However, the DPA determined that in all cases, the appropriate legal basis should be the task carried out in the public interest. Similarly, in Finland, the authority concluded that relying on a legal obligation was not adequate, as the Finnish Education Act lacked specificity and did not mandate the use of digital technologies. Consent was also deemed inappropriate, as data subjects would not be able to provide it freely.

Although the publicly available decision provides limited detail, the case under the Hessian DPA's jurisdiction briefly mentioned that consent should not be used as a legal basis to justify the use of cloud services like Microsoft Office 365 and Google Workspace for Education.

In Spain, the AEPD provided two different opinions on the matter. In one instance, it determined that consent was not suitable as a legal basis for processing students' data, as requested by the complainant, due to the power imbalance between the school and the data subjects. Therefore, the appropriate basis would also be Article 6(1)(e), GDPR. Nonetheless, in another very similar case, the authority did not consider consent as inappropriate but still deemed its use invalid due to the lack of adequate information provided to the data subjects.

The appropriateness of consent was also discussed within the Dutch case, though focused on the processing of data within additional services by Google as a controller, instead of the schools. According to the DPA, consent was also not applicable, as there was also a clear imbalance of power between schools and parents/children, and it would not be freely given.

As described above, most cases indicate that Article 6(1)(e) of the GDPR is the most appropriate legal basis for schools processing data as controllers when deploying Google Workspace for Education. When Google processes personal data for its own purposes, such as within additional services, a new legal relationship with the data subjects must be established, along with a new legal basis. A significant issue remains concerning the data Google accesses solely due to its relationship with schools. If such data is used for purposes like training AI, it raises the question of whether schools could be recognized as joint controllers. This scenario likely falls outside their responsibilities as public entities and, therefore, beyond the scope of Article 6(1)(e).

4.4. Transparency obligations

The provision of information to data subjects under Articles 12–14, GDPR, was also subject to analysis. In Norway, the Municipality in question held a meeting with parents to present information about data processing. However, the DPA was of the opinion that such meetings or merely referring to Google's ToS were insufficient and should be supplemented with more detailed written information, especially considering that the services targeted children.

In Spain, the AEPD found that the documents provided to parents were also insufficient to meet the GDPR's information requirements. Key information was missing, and the documents were not written in a language that children, as data subjects, could understand. Similarly, in Finland, the DPA determined that Google's ToS were too general and difficult to interpret, posing a risk that processing activities were not adequately defined.

It is important to emphasize that Google's ToS establish a binding relationship between the school and Google. When the school acts as a controller, it must provide appropriate information to the data subjects, including details on how it processes student data beyond what was agreed upon with the processor. This information must be presented in a manner that children, as data subjects, can understand.

4.5. Risk assessment on the security of processing and DPIAs

The requirements described so far show how important and yet challenging it can be for educational institutions to assess the risks to the rights of the data subjects involved in the data processing. Most cases discuss the need to carry out a risk assessment on the security of data processing (Article 32, GDPR), and/or a DPIA (Article 35, GDPR).

Regarding the obligations under Article 32 of the GDPR, the Danish DPA concluded that the Helsingør Municipality should have conducted an analysis to identify the potential risks that access to Google Workspace for Education's additional services would entail. In this instance, it pertained to the display of students' personal data when using YouTube. Similarly, in the Norwegian case, the DPA determined that municipalities are responsible for conducting risk assessments under Article 32 when procuring hardware and software for educational use. While some municipalities had them carried out, they were deemed inadequate as the municipalities had not implemented measures to stay informed about the constant changes in Google's ToS.

When it comes to DPIAs, while the specific list of processing activities that are considered high risk differs among DPAs, there is a high degree of convergence in the cases presented above. The Danish DPA determined that a DPIA should have been conducted by the Municipality in question due to the implementation of new and complex technology and the processing of children's data. The authority considered the risk particularly significant due to the implementation of the technology within the educational context, compounded by the fact that other Google products were funded by targeted advertisements and the sale of information. The Norwegian DPA echoed similar concerns, considering the application of new technological or organizational solutions, such as the use of cloud services in primary schools, and the processing of personal data of vulnerable individuals.

The lack of a DPIA constituted the main reason to initiate investigations within the scope of the Swedish DPA. Although a DPIA was carried out when the service was initially implemented in 2014, it was not reviewed when the service was migrated to the controller's own IT environment in 2020. The IMY identified two criteria warranting a DPIA: the large-scale processing of data, and the processing of data concerning vulnerable individuals.

One of the cases brought before the Spanish DPA also highlighted the inadequacy of the conducted DPIA. Despite using a template provided by the authority, the assessment failed to address the unique aspects of the case, particularly the processing of children's data.

Within the Icelandic cases, the decisions varied according to the previous behavior of each municipality. In the case of Kópavogur, the DPIA has been conducted, but it was not regularly updated and did not encompass the latest changes made by Google in the way it process personal data. Reykjavik, Reykjanesbær, Hafnarfjörður and Garðabæjar municipalities have performed DPIAs, but they did not follow all requirements of Article 35, GDPR. This included assessing Google's systems in relation to the data it could use for its own purposes, whether processing operations were necessary and proportionate, as well as the full impact Google Workspace for Education could have on the rights and freedoms of students.

Finally, the Dutch case stands out when it comes to performing DPIAs. Among all the cases examined, this was the most comprehensive, and extensively explored the specificities of the technology. This depth of analysis was only made possible by DPIAs and audits conducted by Privacy Company on behalf of educational institutions. Several risks were only brought to light through them, suggesting that similar issues may have gone unnoticed in the other cases. It also illustrates that conducting well-executed DPIAs is extremely time-consuming and financially demanding, which may not be necessarily feasible for schools in other situations. Additionally, it demonstrates that despite the alterations made by Google following the identification of a first set of risks, these changes led to the need for new assessments, which uncovered additional risks.

Therefore, rather than being a one-time check, DPIAs should be an exercise to be carried out constantly, especially when there are changes in the technological or organizational situation. In a case where the company offers standardized ToS and has the prerogative to change them at any time, schools find themselves in an extremely complicated situation. This prompted the Belgian authority VTC to assert that for schools, conducting DPIAs is not merely difficult but frequently unfeasible. Apart from the shortage of human and financial resources necessary for such undertakings, schools also lack real visibility of the risks posed by the technology. The collaborative decision-making model identified in the Netherlands and Denmark, for example, where human and financial resources were pooled, may be an effective way to address this problem. Furthermore, focusing on technologies over which the state and schools have more control can also help solve it. This will be further discussed in Section 5.

4.6. Data transfers

Data transfers between the EU and third countries can be carried out under certain circumstances defined by Chapter V, GDPR. In the case of the US, this has been historically legitimized by adequacy decisions based on Article 45, GDPR. However, the situation has become increasingly complex over the years, due to invalidations of these arrangements by the CJEU. Two main challenges in this regard were identified by the Court, namely

> (1) a lack of legal safeguards to ensure that any governmental access by the US authorities is necessary and proportionate from the perspective of the EU Charter, considering the substantial interference with EU fundamental rights such governmental access poses; (2) a lack of effective legal remedies for affected data subjects in the EU in order to enable them to access their personal data or to rectify or erase them (Drechsler et al., 2023, p. 5).

In the decisions, the risks associated with transferring data to the US were a recurring topic and although the European Commission have approved a new adequacy decision in July 2023 for the US, all positions discussed here relate to facts that took place before this date. In cases where no adequacy decision is in place, other justifications may be applicable.

In the Dutch case, as stated above, the Privacy Company's 2021 DPIA found that one of the two differences between the free and premium versions of Google Workspace for Education was the option to choose EU data center storage for specific Core Services. Even in these circumstances, however, certain data processing activities, such as providing technical support to users, might still entail transfers to the US.

As a result of the jurisprudence in Schrems-II and of the EDPB measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (EDPB, 2020), schools would need to perform a risk analysis of the transfers outside the EEA. In the Dutch case, uncertainty arose regarding schools' ability to use SCC due to the change of the definition of international transfer in the SCC published by the Commission in 2021. Schools would be required to implement supplementary measures to guarantee compliance with the EU standards for safeguarding personal data. Similar concerns were noted in the Danish, Finnish and Icelandic cases.

The EDPB recommends employing robust encryption as the most effective measure to mitigate the risks associated with unlawful processing when transferring data outside of the EEA. Although the municipality in the Danish case argued that it used encryption when data was transmitted to and processed by Google, it was not considered strong enough by the DPA, as Google could still access the information in plain text. A similar situation occurred in Iceland, where the DPA found that, in certain cases, it could not be ruled out that companies within Google's economic group retained the encryption key, thereby significantly undermining the effectiveness of the encryption in safeguarding data.

5. Data colonialism within Google Workspace for Education

Despite being the protagonist of historical colonialism, Europe is also grappling with the adverse effects of data colonialism. The GDPR and the European Data Strategy stand as clear illustrations of the EU's attempt to guarantee digital sovereignty and pursue a "third way", different from the approaches taken by the US and China.

Considering the focus of the Special Issue in which this article is included—"Education governance, digitalization and the Global South: New actors and methods in local realities"—this paper focuses on presenting how data colonialism has been addressed in the EU, a region with historical privileges that directly impact technologies' sociotechnical affordances. These very privileges have had an important role in how countries within the Global South, and Global Majority more broadly, can actually govern digital technologies in education, as they often have fewer material resources and political power to independently shape its digital destiny and tame the social quantification sector.

The analysis made in this section certainly does not aim to formulate a blueprint for the Global South to follow, as this would only reinforce the consequences of historical colonialism, deepen the Brussels effect and hinder its digital sovereignty even further. Instead, it seeks to present both the merits, but, most importantly, some limitations of positions taken by the select EEA countries. Gaining insight into how other countries around the world address the issue and regulate data governance is important to a) discern what can be factually achieved taking into account their socioeconomic specificities, especially the availability of resources and political power; b) recognize that problems related to data colonialism are global and go beyond the poles of power established in a post-colonial order; and c) learn about the consequences of the decisions made in order to understand the epistemology that underlies them and map out other possible solutions.

The sections above demonstrate that Google Workspace for Education has been the target of authorities' positions for many different reasons, but some patterns can be recognized. The goal of this session is, thus, to identify how data colonialism, in its totalizing and expansionist mission, creates risks for populations around the world that might go beyond compliance with the data protection framework. I will present some patterns encountered in the positions related to the four main components of data colonialism as described in Section 2 and analyze their strengths and weaknesses. I will also introduce the concept of digital sovereignty which, although not directly part of the theoretical framework, intersects with some of the cases discussed above and is linked to potential solutions for tackling data colonialism.

5.1. Appropriation of resources through the lack of compliance with the data protection framework justified by specific narratives

An important aspect of data colonialism is the idea of appropriation of resources. Data are seen as readily available and abundant, much like a natural resource such as oil or minerals. This perspective leads to the perception that data can be harvested, exploited, and used without considering the implications or consequences for the individuals and groups from whom the data is collected. Just as historical colonial powers exploited land, natural resources, and labor from colonized territories, the social quantification sector may similarly exploit data without sufficient regard for people's rights to privacy, data protection, and autonomy.

Viewed through the lens of data commodification, data are perceived as traces left behind by individuals or groups when using technology, as something that naturally exists, representing missed opportunities if not adequately harnessed. However, data is always the result of an abstraction process, one facilitated by specific design choices.

Non-compliance with data protection regulations is an important means to guarantee that more data are available for the company's commercial purposes. Both Google and the public entities using its services have failed to adhere to fundamental rules outlined in the GDPR. This was particularly evident in the Netherlands and Denmark cases, where more comprehensive investigations into the technology's functionality were conducted, either through third-party DPIAs or by the DPAs themselves.

The lack of compliance is generally disguised by very specific narratives that help justify data colonialism, which is also one of its main aspects as highlighted by Couldry and Mejias (2019). Apart from this broader narrative of data commodification, the strategy adopted by Google is related to what Lindh and Nolin (2016) define as a front end/back end strategy. While the service's advantages are evident to users (front end) such as free services and interoperability, the back-end activities are relatively hidden by a specific narrative. The authors have analyzed Google Apps for Education's (now Google Workspace for Education) policy documents and concluded that they had the aim of "disguis[ing] the business model and persuad[ing] the reader to understand Google as a free public service, divorced from marketplace contexts and concerns" (Lindh and Nolin, 2016, p. 650). This is done through many different tactics such as focusing on the benefits for user experience (benefiting rhetoric) and framing practices related to their business model as minor aspects of their activities (side-lining rhetoric). The cases above demonstrate that it also involved using specific language that fosters the perception among users that the information Google collects is not personal data, but "service" data.

5.2. Unequal data relations and global distribution of the benefits of resource appropriation

Apart from the appropriation of resources, justified by specific narratives, data colonialism is also embedded in unequal social-economic relations and unequal global distribution of the benefits of resource appropriation. Although these are two separate components, they can certainly be identified together in the cases described above. Section 3 outlined the main functionalities of Google Workspace for Education and the business model it relies upon. It showed that the data relations between Google, schools, and data subjects are unequal for several reasons.

First, it is important to emphasize that providing digital technology solutions for education is not Googles' main activity. Google's business model is primarily based on data harvesting and targeted advertising. Some view Google's offer of this edtech for free as a genuine act of charity, something the company does to fulfill its social role. While this may indeed be part of a broader justification for its provision, the facts above demonstrate that children's data have been processed for purposes contrary to their best interests. The true intention behind the technology, or the narrative presented by the company, loses significance when such evidence is brought to light.

As discussed above, the way Google Workspace for Education operates, especially when using AI systems, brings about several challenges to the exchange of necessary information between data controllers and processors. It is not easy to identify which data have been used by these systems to draw inferences or make decisions, as well as the weight each piece of data has. Schools generally lack the expertise and resources required to obtain relevant information about their operation, not only to procure the service but also to ensure its compliance with data protection rules and the implementation of children's best interests. The opacity of the operations conducted with personal data, therefore, not only interferes in several rights put forth in the data protection framework, but also increases the power imbalance between schools and edtech providers.

This further emphasizes the influence wielded by the social quantification sector over individuals as a whole. The accumulation of data enables deeper insights to be extracted, thereby amplifying the potential for manipulation by these entities. This is even more problematic when it comes to educational data, which are so valuable within a human profile and so indicative of a country's human capacity and resources.

The power imbalance among the involved actors also results in the benefits of data appropriation being concentrated in the hands of the social quantification sector. Considering the provision of technology by private actors, any crucial insight that can be derived from data collected within education remains restricted to the information that the company is willing to share with the government. Public entities lose the capacity for adequate analysis of the implemented public policy and the use of data for other purposes that might be aligned with children's development and education.

5.3. Digital sovereignty

I have discussed above the key elements of data colonialism, how it manifests, and how it could be identified through the mapping of challenges undertaken in the preceding sections. Although it does not fall directly within the theoretical framework of data colonialism, it is essential to explore the concept of digital sovereignty in greater depth. This concept intersects with some of the cases outlined above and is closely tied to potential solutions for addressing data colonialism.

The German case in Hesse, for instance, gained attention due to Microsoft's announcement that its services would no longer be delivered through a German cloud. This meant that the state's control over the data generated by these services would be affected, and other services, such as Google Workspace for Education, would also need to be reconsidered. In a similar fashion, France decided that Microsoft and other cloud services like Google do not comply with its Cloud at the Center doctrine, and their provision of free services would not only impact competition, but also be contrary to French public procurement rules. The Danish, Dutch, and Finish cases relied on digital sovereignty arguments while focusing on Google Workspace for Education's compliance with data transfer requirements outlined in the GDPR, particularly in light of the latest developments on this matter within the CJEU.

Indeed, discussing digital sovereignty solely through the lens of competition, procurement, data localization and data transfers can be narrow, and other aspects of this concept should be highlighted. After providing a brief definition of and discussing the concept, I will analyze additional elements that could have also been identified in these cases, which can also be significant for the development of digital sovereignty policies within Global South countries.

5.3.1. The concept of digital sovereignty

The modern concept of national sovereignty is based on an analogue word, and encompasses the power exercised by the state on all affairs within its territory, such as its resources and people. The digital environment, however, puts tension on this concept, as it lacks physical boundaries and is mostly subjected to private forces, especially multinational corporations, which makes it increasingly globalized (Floridi, 2020, p. 372). Therefore, rather than being just a subcategory of sovereignty, digital sovereignty affects the core of political institutions and their very ability to exercise sovereignty (Smuha, 2023, p. 3).

Digital sovereignty can be understood as the “control of the digital”, i.e., the ability not only “to influence [it] (e.g. its occurrence, creation, or destruction), [but also] its dynamics (e.g. its behaviour, development, operations, interactions), including the ability to check and correct for any deviation from such influence” (Floridi, 2020, p. 371). This could be understood in relation to individuals and their ability to shape the digital sphere in a self-determined way or in relation to states (Herlo et al., 2023; Núcleo de Tecnologia do MTST, 2023).

In the case of states, this can occur in two ways. First, by controlling the digital infrastructure, which includes capital resources (such as software, hardware, standards and cables); intellectual resources (such as human resources and institutions); and financial resources to experiment and design new models and possibilities (Pinto, 2018, p. 17). Second, by controlling a country’s destiny through public policies (Lefèvre, 2023) and norm-setting capacity (Smuha, 2023, p. 8).

The control of digital infrastructure is a difficult one, and will depend on the policies, political power, international pressure and influences, as well as resources available to each country. It requires understanding that allocation of resources to this area is essential for the very existence of democracy and people power. This is enough to demonstrate how dangerous and detrimental short-term policies like accepting free services from foreign technology companies with data-driven business models can be. However, considering the broader context also involves recognizing that some countries have limited choices.

Policies focused on the adoption of open-source software, for example, can be an interesting path in the case of countries with few resources, as in addition to being free, these software are more open to public scrutiny. However, this alone is insufficient to build a robust digital policy in a given country. This inadequacy arises not only due to the need for a focus on sustainability and mass adoption but also because of the lobbying and influence of private actors and foreign states in public policies. This demonstrates how the two types of control in digital sovereignty—economic and normative—are interconnected (Pinto, 2018, p. 21; Smuha, 2023).

The relationship between companies and states is also asymmetric in the digital age, with the latter frequently depending on the infrastructure provided by the former. Companies are the ones currently determining the nature and speed of technological change, while states’ role is often perceived as being able to *control* its direction (Floridi, 2020, p. 371). However, this has not been the case for most countries, which already struggle to set this direction and define clear objectives, let alone innovate and proactively consider what kind of technology serves best the public good and aligns with state’s strategies, such as through procurement mechanisms (Mazzucato, 2019, 2020).

Controlling a country’s or even a supranational entity like the EU’s digital destiny through regulation can also be extremely challenging in a globalized world. This includes dealing, for example, with the intense lobbying of tech companies and foreign states in the definition and drafting of policies, as well as in proposing specific legislation related to the digital domain. Defining digital strategies through policy can, for instance, be deeply influenced by consultancy firms, which are increasingly moving from the sidelines to the center of important decisions within the public sphere. Their business models, potential conflicts of interest and lack of transparency are ever more a challange to our democracies and economies (Corporate Europe Observatory, 2023; Mazzucato and Collington, 2023).

The AI Act serves as an important example of the influence on the legislative activities themselves. A report published by Corporate Europe Observatory, for example, showed how the EU’s pioneering attempt to regulate AI has faced intense lobbying from US tech companies. This happened not only through pressure by the corporations themselves, but also through covert groups, tech-funded experts and the US Government (Schyns, 2023). These activities have been ongoing since the initial drafting of the act, and previous research indicates that this is not an isolated case (Bank et al., 2021). Even when legislators are able to pass regulations, the latter are still limited, not only because of possible poor choices while legislating, but also because of the interference from corporate actors and foreign states, as well as the difficulties related to their enforcement (Massé, 2022; Smuha, 2023). Therefore, more than regulating technology, it is important to actually regulate the *incentives* to undermine regulation, especially in strategic sectors such as education. This could include, for instance, implementing a blanket ban on targeted advertising based on the profiling of personal data for all users (regardless of age or the type of personal data, as outlined in the DSA) (Danish Government’s Expert Group on Big Tech, 2023), and regulating the widespread data-driven business model more broadly.

Strengthening digital sovereignty is certainly not linked to anachronic notions of digital sovereignism or digital statism, though. It does not involve replacing a nation’s sovereignty but, rather, seeks to complement it with a contemporary digital counterpart. This kind of digital sovereignty serves as a crucial enabling factor to sovereignty in general, offering a broader array of advantages, such as harmonization (including standards and requirements), ensuring a fair competitive environment, and fostering greater opportunities for coordination among all stakeholders (Floridi, 2020, p. 375).

5.3.2. *A broader understanding of digital sovereignty*

To expand the scope of digital sovereignty beyond the parameters delineated in the positions described above, we can identify interesting elements that go beyond competition, procurement aspects and data localization/data transfer concerns.

The first factor is the existence of resources that enabled actual enforcement and facilitated negotiations with Google, which led to changes in contracts. In the case of the Netherlands, for example, cooperatives of schools and universities, together with other actors, were able to engage Big Tech in months of highly technical discussions based on several DPIAs and deep analysis of the technology. This indicates the existence of capital and intellectual resources to at least understand what was actually happening to personal data. The symbolic power of the Dutch DPA also counted a lot, as some even consider that certain US firms now view the Dutch endorsement as a prestigious status symbol, as a seal of approval that they have navigated one of Europe’s most rigorous data protection compliance procedure (Singer, 2023).

Secondly, a centralized approach was key to enhance their bargaining power and making the solution scalable. They have demonstrated that this is possible not only by centralizing procurement activities within a specific entity, but through cooperatives of schools and universities. Most schools would not have the means, power, and expertise to independently audit technologies, so cooperatives represent their collective interest and preserve, at the same time, some of their autonomy. The same centrality through cooperatives was identified in the Danish case. One of the cases that took place in Germany, on the other hand, demonstrates the imbalance of power and the need for collective approaches. A student in Dortmund refused to use Google Workspace for Education due to privacy concerns, but faced technical and discriminatory issues within the school.

However, it is necessary to consider that focusing on the strategies above alone, while extremely important and demonstrating that adequate enforcement of the GDPR is possible, may not be sufficient to ensure that education is delivered in the best interests of children and in a way that guarantees digital sovereignty.

These negotiations also do not solve the core issue of the data commodification/data flow paradigm (Ducuing, 2020; Purtova and

Maanen, 2023) and the market incentives related to the business model of big tech platforms. Children get used to these platforms and are continuously subjected to surveillance as soon as they leave the controlled school environment. The persistence of the business model and incentives for massive data collection also means that new risks can arise continuously, as was highlighted in the most recent DPIA conducted in the Netherlands. The case of France, in this sense, is quite interesting not only because it bans technologies based on a digital sovereignty perspective, but also because the decision was taken by the Minister of Education and Youth. The possibility to make decisions based on political considerations beyond the data protection framework (which is more challenging when the case is handled by DPAs) allows for a broader range of factors to be taken into account.

Finally, entrusting crucial digital infrastructures to private entities often involves surrendering education-related data that could be used by governments and the civil society in the best interests of children, such as to develop privacy-preserving solutions, as well as innovative and collaborate solutions to improve learning (Hooper et al., 2022, p. 56).

This is where digital sovereignty intersects with the imperative to challenge data universalism. We have observed how issues stemming from datafication, particularly certain business models, are systemic and global in nature. However, endeavors to identify solutions must consistently account for local specificities, encompassing both the material and cultural dimensions of knowledge production. It is essential to harness the full potential of each society, foster new imaginaries, and conceive alternatives for the digital future we aspire to build.

6. Conclusion

Google Workspace for Education is used worldwide by millions of students, and its application has been particularly expanded during the COVID-19 pandemic. Google's educational approach, more strictly focused on the development of skills and competencies, especially for the job market, establishes a digital environment that does not necessarily accommodate divergent pedagogical methodologies. This vision smoothly aligns with the datafication and quantification of education, which brings about several challenges to the protection of children's personal data.

This paper sought to analyze recent positions from EEA authorities related to the use of Google Workspace for Education by public schools. I focused on examining the primary areas of conflict with data protection laws, as well as how they intersect with data colonialism. This analysis exposes not only a consistent failure of schools and Google Workspace for Education to adhere to the data protection framework, but also issues that transcend regulatory compliance.

The positions from public authorities show the inherent challenges posed by the adopted business model, despite efforts made during negotiations to ensure compliance. Even if children's data are not processed for target advertising, they may still be leveraged for other commercial purposes not necessarily aligned with their best interests. Additionally, children are familiarized and nudged to continue using these technologies outside the school environment and throughout their lives. This highlights the importance of discussing the existing incentives for private entities to unlawfully process data, as well as the purposes for which we, as a society, would like children's data to be processed.

I have also discussed how a comprehensive understanding of digital sovereignty should extend beyond competition and data localization/transfer matters. The positions illustrate how the economic and political capital of the analyzed countries significantly influence their level of digital sovereignty, and, consequently, the decisions they can make in practice. While stronger enforcement of the GDPR remains crucial, it alone may not suffice to deliver education in the best interests of children and ensure digital sovereignty, at both individual and collective levels.

Despite the EU's ongoing efforts to implement its data strategy and continuously expand its digital rulebook, it is still necessary to discuss the core essence of digital sovereignty and the underlying causes of the problems these policies try to solve. In light of the Brussels effect, their ramifications must be carefully weighed, justifying global dialogues on digital sovereignty that effectively support individuals and communities beyond the confines of countries, blocs, and companies. There is, therefore, a pressing need to challenge data universalism and collaboratively devise solutions for global issues while accounting for local specificities and exploring alternative approaches to shape the society we aspire to be part of.

Conflicts of interest statement

None.

Funding

This work was supported by the Fonds Wetenschappelijk Onderzoek (FWO) [G0D0622N, 2022].

CRediT authorship contribution statement

Elora Raad Fernandes: Writing – review & editing, Writing – original draft, Methodology, Investigation, Conceptualization,

References

AEPD. (2023a). Resolución de Procedimiento Sancionador. Expediente N.o EXP202102527. ⟨https://www.aepd.es/documento/ps-00176-2022.pdf⟩.

AEPD. (2023b). Resolución de Procedimiento Sancionador. Expediente N.º EXP202104450.

AEPD. (2023c). Resolución de Recurso de Reposición. Expediente N.o EXP202104450. ⟨https://www.aepd.es/documento/reposicion-ps-00334-2022.pdf⟩.

Allen, S., 2022. How a culture of listening can drive digital transformation. Forbes. ⟨https://www.forbes.com/sites/forbesbusinesscouncil/2022/09/09/how-a-culture-of-listening-can-drive-digital-transformation/⟩. September 9.

AP, 2021. Advies Autoriteit Persoonsgegevens (AP) aan SURF en SIVON inzake Google G Suite for Education. Tweede Kamer der State - Generaal. ⟨https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id= 2021Z10202&did= 2021D22378⟩.

Arora, P., 2016. The bottom of the data pyramid: big data and the Global South. Int. J. Commun. 10, 1681–1699. ⟨https://ijoc.org/index.php/ijoc/article/view/4297/1616⟩.

Arora, P., 2019. General data protection regulation—a global standard? Privacy futures, digital activism, and surveillance cultures in the Global South. Surveill. Soc. 17 (5), 717–725. https://doi.org/10.24908/ss.v17i5.13307.

Assemblée Nationale. (2022a). 16ème législature. Question N° 971 de M. Philippe Latombe (Démocrate (MoDem et Indépendants) - Vendée) Question écrite. ⟨https://questions.assemblee-nationale.fr/q16/16-971QE.htm⟩.

Assemblée Nationale. (2022b). Numérique. Gratuité d'Office 365. In Débats Parlementaires. Journal Officiel de La République Française. Constitution du 4 Octobre 1958. 16e Législature. Questions remises à la présidence de l'Assemblée nationale. Réponses de ministres aux questions écrites (Issue 34). ⟨https://questions.assemblee-nationale.fr/static/16/questions/jo/jo_anq_202234.pdf⟩.

Bank, M., Duffy, F., Leyendecker, V., & Silva, M. (2021). The Lobby Network: Big Tech's Web of Influence in the EU. ⟨https://corporateeurope.org/sites/default/files/2021-08/The%20lobby%20network%20-%20Big%20Tech%27s%20web%20of%20influence%20in%20the%20EU.pdf⟩.

Barassi, V., 2020. CHILD | DATA | CITIZEN: Vol. E-book. MIT Press.

Borne, É . (2023, June 1). Actualisation de la doctrine d'utilisation de l'informatique en nuage par l'État (« cloud au centre»). ⟨https://www.legifrance.gouv.fr/circulaire/id/45446?fonds=CIRC&page= 1&pageSize= 10&query=cloud&searchField=ALL&searchType=ALL&tab_selection=all&typePagination=DEFAULT⟩.

Bradford, A., 2020. The Brussels Effect: How the European Union Rules the World. Oxford University Press, Oxford.

Cohen, J.E., 2019. Between Truth and Power: The Legal Constructions of Informational Capitalism. Oxford University Press.

Corporate Europe Observatory. (2023, April 26). How the Commission outsourced its merger policy to Google's best friend. ⟨https://corporateeurope.org/en/2023/04/how-commission-outsourced-its-merger-policy-googles-best-friend⟩.

Couldry, N., Dijck, J. van, 2015. Researching social media as if the social mattered. Soc. Media Soc. 1 (2). https://doi.org/10.1177/2056305115604174.

Couldry, N., Mejias, U.A., 2019. The Costs of Connection: How Data is Colonising Human Life and Appropriating it for Capitalism. Standard University Press.

Danish Government's Expert Group on Big Tech. (2023, July). Democratic control over big tech business models. ⟨https://www.eng.em.dk/Media/638429880879563320/(eng)-ekspertgruppe_demokratisk%20kontrol_060723.pdf⟩.

Datatilsynet - Danish Data Protection Authority. (2021, September 10). Alvorlig kritik af Helsingør Kommune i Chromebook-sag. ⟨https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/sep/afgoerelse-vedroerende-brud-paa-persondatasikkerheden⟩.

Datatilsynet - Danish Data Protection Authority. (2022a, July 14). Datatilsynet nedlægger behandlingsforbud i Chromebook-sag. ⟨https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/jul/datatilsynet-nedlaegger-behandlingsforbud-i-chromebook-sag⟩-.

Datatilsynet - Danish Data Protection Authority. (2022b, August 18). Datatilsynet fastholder forbud i Chromebook-sag. ⟨https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/aug/datatilsynet-fastholder-forbud-i-chromebook-sag⟩.

Datatilsynet - Danish Data Protection Authority. (2022c, August 19). Konstruktivt møde om Chromebooks. ⟨https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/aug/konstruktivt-moede-om-chromebooks⟩.

Datatilsynet - Danish Data Protection Authority. (2022d, September 8). Chromebooks: Datatilsynet suspenderer forbud og giver påbud om lovliggørelse.

Datatilsynet - Danish Data Protection Authority. (2022e, November 4). Datatilsynet undersøger kommuners materiale om Google Workspace. ⟨https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/nov/datatilsynet-undersoeger-kommuners-materiale-om-google-workspace⟩.

Datatilsynet - Danish Data Protection Authority. (2022f, December 13). Yderligere materiale udsætter afgørelse om Chromebooks. ⟨https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/dec/yderligere-materiale-udsaetter-afgoerelse-om-chromebooks⟩.

Datatilsynet - Danish Data Protection Authority, 2024, January 30. Datatilsynet giver påbud i Chromebook-sag. ⟨https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/jan/datatilsynet-giver-paabud-i-chromebook-sag⟩.

Datatilsynet - Norwegian Data Protection Authority. (2020a). Varsel om vedtak om irettesettelse - Bruk av G Suite for Education - Sandnes Kommune. ⟨https://www.datatilsynet.no/contentassets/ff4de39da1174e7bb144d7a96027922c/varsel-om-vedtak-om-irettesettelse—bruk-av-g-suite-for-education—sandnes.pdf⟩.

Datatilsynet - Norwegian Data Protection Authority. (2020b). Varsel om vedtak om irettesettelse - Bruk av Google Chromebook i skolen - Strand Kommune. ⟨https://www.datatilsynet.no/contentassets/ff4de39da1174e7bb144d7a96027922c/varsel-om-vedtak-om-irettesettelse—bruk-av-google-chromebook-i-skolen—strand.pdf⟩.

Datatilsynet - Norwegian Data Protection Authority. (2020c). Varsel om vedtak om irettesettelse - Bruk av Google Chromebook og G Suite for Education i skolen - Bergen Kommune. ⟨https://www.datatilsynet.no/contentassets/ff4de39da1174e7bb144d7a96027922c/varsel-om-vedtak-om-irettesettelse—bruk-av-google-chromebook-og-g-suite-for-education—bergen2.pdf⟩.

Datatilsynet - Norwegian Data Protection Authority. (2020d, December 11). Bruk av Google Chromebook og G Suite for Education (og andre skytjenester) i grunnskolen. ⟨https://www.datatilsynet.no/personvern-pa-ulike-omrader/skole-barn-unge/bruk-av-google-chromebook-og-g-suite-for-education-og-andre-skytjenester-i-grunnskolen/⟩.

Datatilsynet - Norwegian Data Protection Authority. (2020e, December 11). Varsel om irettesettelse for feil bruk av Googles løsninger i skolen. ⟨https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/varsel-om-irettesettelse-for-feil-bruk-av-googles-losninger-i-skolen/⟩.

Dedezade, E., 2018. Microsoft to deliver cloud services from new datacentres in Germany in 2019 to meet evolving customer needs. Microsoft Stories Eur. ⟨https://news.microsoft.com/europe/2018/08/31/microsoft-to-deliver-cloud-services-from-new-datacentres-in-germany-in-2019-to-meet-evolving-customer-needs/⟩.

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit. (2019a, July 9). Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Microsoft Office 365 in hessischen Schulen. ⟨http://web.archive.org/web/20191220095453/https:/datenschutz.hessen.de/pressemitteilungen/stellungnahme-des-hessischen-beauftragten-f%C3%BCr-datenschutz-und⟩.

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit. (2019b, August 2). Zweite Stellungnahme zum Einsatz von Microsoft Office 365 in hessischen Schulen. ⟨http://web.archive.org/web/20221203045150/https:/datenschutz.hessen.de/pressemitteilungen/zweite-stellungnahme-zum-einsatz-von-microsoft-office-365-hessischen-schulen⟩.

Dinum. (n.d.). Le Cloud pour les administrations. Retrieved September 27, 2023, from ⟨https://www.numerique.gouv.fr/services/cloud/doctrine/⟩.

Drechsler, L., Elbi, A., Kindt, E., Kun, E., Meszaros, J., & Vranckaert, K. (2023). CiTiP Working Paper Series. Third time is the charm? The draft Data Privacy Framework for international personal data transfers from the European Union to the United States. ⟨https://www.law.kuleuven.be/citip/en/docs/books/citip-working-paper-2023-drechsler-elbi-kindt-kun.pdf⟩.

Ducuing, C., 2020. Beyond the data flow paradigm: governing data requires to look beyond data. Technol. Regul. 57–64. https://doi.org/10.26116/techreg.2020.006.

EDPB. (2020). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Version 2.0. ⟨https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf⟩.

EDPB. (2021). Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 2.1.

Fader, P., Hoyne, N., 2021. Important lessons for embracing customer lifetime value. Think. Google. ⟨https://www.thinkwithgoogle.com/marketing-strategies/data-and-measurement/customer-lifetime-value/?utm_source=rss-reader&utm_medium=rss&utm_campaign=rss-feed⟩.

Fahey, E., 2022. The EU as a Global Digital Actor: Institutionalising Global Data Protection, Trade, and Cybersecurity Oxford. Hart Publishing. https://doi.org/10.5040/9781509957071.ch-001.

Floridi, L., 2020. The fight for digital sovereignty: what it is, and why it matters, especially for the EU. Philos. Technol. 33 (3), 369–378. https://doi.org/10.1007/s13347-020-00423-6.

GDPR Enforcement Tracker. (2024). ⟨https://www.enforcementtracker.com/⟩.

GDPR Hub. (2024). ⟨https://gdprhub.eu/⟩.

Gleason, H., Heath, B.K., 2021. Injustice embedded in Google Classroom and Google Meet: a techno-ethical audit of remote educational technologies. Ital. J. Educ. Technol. 29 (2), 26–41. https://doi.org/10.17471/2499-4324/1209.

Google, 2006. Google Announces Education News at Educause. News from Google. ⟨http://googlepress.blogspot.com/2006/10/google-announces-education-news-at_10.html⟩.

Google, 2020. Introducing Google Workspace and a new set of offerings to better meet your needs. Google Work. Updates. ⟨https://workspaceupdates.googleblog.com/2020/10/introducing-google-workspace.html⟩.

Google, 2023a. Choose the right edition for your institution. Google for Education. ⟨https://edu.google.com/workspace-for-education/editions/compare-editions/⟩.

Google, 2023b. Compare Google Workspace editions. Google Workspace Admin Help. ⟨https://support.google.com/a/answer/6043385?hl=en&co=DASHER._Family%3DEducation⟩.

Google, 2023d. Google workspace for education core and additional services. Google Workspace Admin Help. ⟨https://support.google.com/a/answer/6356441?hl=en⟩.

Google, 2023e. Make learning more alive with Jamboard. Google for Education. ⟨https://edu.google.com/jamboard/⟩.

Google, 2023c. Find the best Chromebook for your institution. Google for Education. ⟨https://edu.google.com/intl/ALL_us/chromebooks/find-a-chromebook/⟩.

Grondwettelijk Hof. (2023). Arrest nr. 26/2023 van 16 februari 2023. Rolnummers: 7494, 7505, 7526 en 7606. 2023. ⟨https://www.const-court.be/public/n/2023/2023-026n.pdf⟩.

Herlo, B., Ullrich, A., & Vladova, G. (2023). Sustainable Digital Sovereignty: Interdependencies Between Sustainable Digitalization and Digital Sovereignty. https://doi.org/10.34669/WI.WS/32.

Hessel, S., 2022. FAQ about telemetry and diagnostic data in Microsoft 3. , September 17 65. Reusch Law. ⟨https://www.reuschlaw.de/en/news/faq-about-telemetry-and-diagnostic-data-in-microsoft-365/⟩. , September 17.

Hogan, A., Thompson, G., 2021. Introduction: the “publicness” of schooling. Privatisation and Commercialisation in Public Education: How the Public Nature of Schooling in Changing. Routledge.

Holmes, W. (2023). The unintended consequences of artificial intelligence. ⟨https://www.ei-ie.org/en/item/28115:the-unintended-consequences-of-artificial-intelligence-and-education⟩.

Hooper, L., Livingstone, S., & Pothong, K. (2022). Problems with data governance in UK schools: the cases of Google Classroom and ClassDojo. ⟨https://digitalfuturescommission.org.uk/wp-content/uploads/2022/08/Problems-with-data-governance-in-UK-schools.pdf⟩.

Human Rights Watch. (2022). “How dare they peep into my private life?”: Children’s Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic.

IMY. (2023a). Beslut efter tillsyn enligt dataskyddsförordningen - Barn- och utbildningsnämnden i Östersunds kommun. ⟨https://www.imy.se/globalassets/dokument/beslut/2023/beslut-om-tillsyn-barn-och-utbildningsforvaltningen-ostersunds-kommun.pdf⟩.

IMY. (2023b, November 30). Sanktionsavgift mot kommun som inte bedömt konsekvenser innan Google Workspace infördes. ⟨https://www.imy.se/nyheter/sanktionsavgift-mot-kommun-som-inte-bedomt-konsekvenser-innan-google-workspace-infordes/⟩.

Kiecza, D., 2022. Practice sets: a more personal path to learning. , March 16 Google - Keyword. ⟨https://blog.google/outreach-initiatives/education/introducing-practice-sets/⟩. , March 16.

Kimery, A., 2024. Google settles over kids’ biometric data collection in schools. , August 1 Biom. Update. ⟨https://www.biometricupdate.com/202408/google-settles-over-kids-biometric-data-collection-in-schools⟩. , August 1.

Kucirkova, N., Brod, G., Gaab, N., 2023. Applying the science of learning to EdTech evidence evaluations using the EdTech Evidence Evaluation Routine (EVER). npj Sci. Learn. 8 (1), 35. ⟨https://www.nature.com/articles/s41539-023-00186-7⟩.

La Chambre des Représentants. (2023). Question et réponse écrite n° 55-473: Accord de coopération entre l’APD et la VTC. ⟨https://www.stradalex.com/nl/sl_src_publ_div_be_chambre/document/QRcrb_55-b107-1263-0473-2022202319113⟩.

Langreo, L., 2023. Google executive: AI could ‘transform’ school into a ‘personal learning experience’. Education Week. ⟨https://www.edweek.org/technology/google-executive-ai-could-transform-school-into-a-personal-learning-experience/2023/07⟩.

Laval, C., 2019. A escola não é uma empresa: o neoliberalismo em ataque ao ensino público. Boitempo.

Lawn, M., 2013. Voyages of measurement in education in the twentieth century: experts, tools and centres. Eur. Educ. Res. J. 12 (1), 108–119. https://doi.org/10.2304/eerj.2013.12.1.108.

Lazare, M., 2021a. A peek at what’s next for Google Classroom. Keyword. ⟨https://blog.google/outreach-initiatives/education/classroom-roadmap/⟩.

Lazare, M., 2021b. Learning with Google. Google YouTube Channel 2021. ⟨https://youtu.be/oGEy4PfcdZ8?t= 2449⟩.

Lefèvre, F. (2023, March 11). Soberania e Segurança negligenciadas. Flávia Lefèvre: Liberdade e Direitos Na Internet e Nas Telecomunicações. ⟨https://flavialefevre.com.br/pt/soberania-e-seguranca-negligenciadas⟩.

Lima, S. (Ed.). (2020). Educação, dados e plataformas: análise descritiva dos termos de uso G Suite for Education e Microsoft 365 (pp. 11–12). São Paulo: Iniciativa Educação Aberta. ⟨https://zenodo.org/records/4012539#.X1EOdpNKi-4⟩.

Lindh, M., Nolin, J., 2016. Information we collect: surveillance and privacy in the implementation of Google apps for education. Eur. Educ. Res. J. 15 (6), 644–663. https://doi.org/10.1177/1474904116654917.

Magalhães, J.C., Couldry, N., 2021. Giving by taking away: big tech, data colonialism, and the reconfiguration of social good. Int. J. Commun. 15, 343–362. ⟨https://ijoc.org/index.php/ijoc/article/view/15995/3322⟩.

Magid, L., 2014. Google classroom offers assignment center for students and teachers. Forbes. ⟨https://www.forbes.com/sites/larrymagid/2014/05/06/google-classroom-offers-control-center-for-students-and-teachers/⟩.

Marrafon, M.A., Fernandes, E.R., 2020. A, B, C, Google: Riscos ao direito fundamental à proteção de dados de crianças e adolescentes no G Suite for Education. Rev. Direito Público 17 (95), 202–229.

Massé, E. (2022). Four Years Under the EU GDPR: How to Fix its Enforcement. ⟨https://www.accessnow.org/wp-content/uploads/2022/07/GDPR-4-year-report-2022.pdf⟩.

Mazzucato, M. (2019). Governing Missions in the European Union. https://doi.org/10.2777/014023.

Mazzucato, M. (2020). Mission-oriented public procurement: international examples. ⟨https://www.ucl.ac.uk/bartlett/public-purpose/sites/public-purpose/files/final_mission-oriented_public_procurement_international_examples.pdf⟩.

Mazzucato, M., Collington, R., 2023. The Big Con: How the Consulting Industry Weakens Our Businesses, Infantilizes Our Governments, and Warps Our Economies. Penguin Press.

Ministerie Van Onderwijs, Cultuur en Wetenschap. (2023). Stand van zaken DPIA Google Workspace for Education. ⟨https://www.rijksoverheid.nl/documenten/kamerstukken/2023/04/20/stand-van-zaken-dpia-google-workspace-for-education⟩.

Mosco, V., 2017. Becoming Digital: Toward a Post-Internet Society. Emerald Publishing.

mrtee. (2023a, March 24). Dortmunder Gymnasium erhält Weisung der Bezirksregierung, die Nutzung von Google Workspace for Education einzustellen. ⟨https://news.datenschutz-schule.info/2023/03/24/dortmunder-gymnasium-erhaelt-weisung-der-bezirksregierung-die-nutzung-von-google-workspace-for-education-einzustellen/⟩.

mrtee. (2023b, July 26). Beschluss des OVG NRW zum Google Workspace for Education Fall veröffentlicht. Datenschutz – Schule – News. ⟨https://news.datenschutz-schule.info/2023/07/26/beschluss-des-ovg-nrw-zum-google-workspace-for-education-fall-veroeffentlicht/⟩.

Nas, S. (2021, August 9). Google mitigates 8 high privacy risks for Workspace for Education. ⟨https://www.privacycompany.eu/blogpost-en/google-mitigates-8-high-privacy-risks-for-workspace-for-education⟩.

Nas, S., Terra, F., 2021a. DPIA on the use of Google G Suite (Enterprise) for Education. Univ. Gron. Amst. Univ. Appl. Sci. ⟨https://www.surf.nl/files/2021-06/updated-g-suite-for-education-dpia-12-march-2021.pdf⟩.

Nas, S., & Terra, F. (2021b). Update DPIA report Google Workspace for Education 2 August 2021. ⟨https://www.surf.nl/files/2021-08/update-dpia-report-2-august-2021.pdf⟩.

Nas, S., Terra, F., 2023. Verification report Google remediation measures Workspace for Education. SURF SIVON. ⟨https://sivon.nl/wp-content/uploads/2023/07/20230724-clean-Workspace-for-Education.pdf⟩.

Núcleo de Tecnologia do MTST. (2023). Homeless Worker Movement in Brazil and the struggle for digital sovereigtny. ⟨https://nucleodetecnologia.com.br/docs/Cartilha-MTSTec-ENG.pdf⟩.

Organization for Economic Cooperation and Development (OECD), 2021. OECD Digital Education Outlook 2021. Pushing the frontiers with AI, blockchain, and robots. OECD Publishing. https://doi.org/10.1787/589b283f-en.

Patil, L., 2023. The business of development: the institutional rationales of technology corporations in educational development. Int. J. Educ. Dev. 97. https://doi.org/10.1016/j.ijedudev.2022.102712.

Perez, S., 2015. Google expands its educational platform "Classroom" with a new API, share button for websites. Tech. Crunch. ⟨https://techcrunch.com/2015/06/29/google-expands-its-educational-platform-classroom-with-a-new-api-share-button-for-websites/⟩.

Perez, S., Lardinois, F., 2016. Google rebrands its business apps as G Suite, upgrades apps & announces Team Drive. Tech Crunch. ⟨https://techcrunch.com/2016/09/29/google-rebrands-its-business-apps-as-g-suite-launches-team-drive-upgrades-apps/⟩.

Perrotta, C., Gulson, K.N., Williamson, B., Witzenberger, K., 2021. Automation, APIs and the distributed labour of platform pedagogies in Google Classroom. Crit. Stud. Educ. 62 (1), 97–113. https://doi.org/10.1080/17508487.2020.1855597.

Persónuvernd. (2023a, December 6). Úttekt á notkun Garðabæjar á skýjalausn Google í grunnskólastarfi. Mál nr. 2022020418. ⟨https://www.personuvernd.is/urlausnir/uttekt-a-notkun-gardabaejar-a-skyjalausn-google-i-grunnskolastarfi⟩.

Persónuvernd. (2023b, December 6). Úttekt á notkun Hafnarfjarðarbæjar á skýjalausn Google í grunnskólastarfi. Mál nr. 2022020415. ⟨https://www.personuvernd.is/urlausnir/uttekt-a-notkun-hafnarfjardarbaejar-a-skyjalausn-google-i-grunnskolastarfi⟩.

Persónuvernd. (2023c, December 6). Úttekt á notkun Kópavogsbæjar á skýjalausn Google í grunnskólastarfi. Mál nr. 2022020414. ⟨https://www.personuvernd.is/urlausnir/uttekt-a-notkun-kopavogsbaejar-a-skyjalausn-google-i-grunnskolastarfi⟩.

Persónuvernd. (2023d, December 6). Úttekt á notkun Reykjanesbæjar á skýjalausn Google í grunnskólastarfi. Mál nr. 2022020416. ⟨https://www.personuvernd.is/urlausnir/uttekt-a-notkun-reykjanesbaejar-a-skyjalausn-google-i-grunnskolastarfi⟩.

Persónuvernd. (2023e, December 6). Úttekt á notkun Reykjavíkurborgar á skýjalausn Google í grunnskólastarfi. Mál nr. 2022020363. ⟨https://www.personuvernd.is/urlausnir/uttekt-a-notkun-reykjavikurborgar-a-skyjalausn-google-i-grunnskolastarfi⟩.

Pinto, R.Á., 2018. Digital sovereignty or digital colonialism? Sur 15 (27), 15–27. ⟨https://sur.conectas.org/soberania-digital-ou-colonialismo-digital/⟩.

Poortvliet, J., 2018. Microsoft and Telekom no longer offer cloud storage under German jurisdiction. Nextcloud. ⟨https://nextcloud.com/blog/microsoft-and-telekom-no-longer-offer-cloud-storage-under-german-jurisdiction/⟩.

Privacy Company. (2021a, February 23). Privacy assessment Google Workspace (G Suite) Enterprise: Dutch government consults Dutch Data Protection Authority on high privacy risks. ⟨https://www.privacycompany.de/blogpost-en/privacy-assessment-google-workspace-g-suite-enterprise-dutch-government-consults-dutch-data-protection-authority-on-high-privacy-risks⟩.

Privacy Company. (2021b, September 8). Google mitigates 8 high privacy risks for Workspace for Education. ⟨https://www.privacycompany.eu/blogpost-en/google-mitigates-8-high-privacy-risks-for-workspace-for-education⟩.

Purtova, N., Maanen, G. van, 2023. Data as an economic good, data as a commons, and data governance. Law, Innov., Technol. (Adv. Online Publ.) 16 (1). https://doi.org/10.48550/arXiv.2212.10244.

Sato, M., 2024. Google confirms the leaked Search documents are real. Verge. ⟨https://www.theverge.com/2024/5/29/24167407/google-search-algorithm-documents-leak-confirmation⟩.

Schyns, C. (2023). The Lobbying Ghost in the Machine: Big Tech's covert defanging of Europe's AI Act. ⟨https://corporateeurope.org/sites/default/files/2023-03/The%20Lobbying%20Ghost%20in%20the%20Machine.pdf⟩.

Singer, N., 2017. How Google took over the classroom. The New York Times. ⟨nytimes.com/2017/05/13/technology/google-education-chromebooks-schools.html⟩.

Singer, N., 2023. How the Netherlands is taming big tech. The New York Times. ⟨https://www.nytimes.com/2023/01/18/technology/dutch-school-privacy-google-microsoft-zoom.html⟩.

Singer, N., Wakabayashi, D., 2020. New Mexico sues Google over children's privacy violations. The New York Times. ⟨https://www.nytimes.com/2020/02/20/technology/new-mexico-googlelawsuit.html⟩.

Sinha, S., 2023. New Google for Education tools for how you teach, learn and manage. Google - Keyword. ⟨https://blog.google/outreach-initiatives/education/google-for-education-iste-2023/⟩.

Sinha, S., 2024. New education features to help teachers save time and support students. Google - Keyword. ⟨https://blog.google/outreach-initiatives/education/bett-2024-google-for-education-updates/⟩.

Smuha, N.A., 2023. Digital sovereignty in the European Union: five challenges from a normative perspective. Work. Pap. - ERA Conf. Proc. https://doi.org/10.2139/ssrn.4501591.

SURF. (2021a, February 22). SURF and SIVON discuss privacy risks with Google. ⟨https://www.surf.nl/en/surf-and-sivon-discuss-privacy-risks-with-google⟩.

SURF. (2021b, July 8). Agreement with Google on privacy risks. ⟨https://www.surf.nl/en/agreement-with-google-on-privacy-risks⟩.

SURF. (2023a, April 20). Status of Google Workspace DPIA: update on privacy measures. ⟨https://www.surf.nl/en/status-of-google-workspace-dpia-update-on-privacy-measures⟩.

SURF. (2023b, May 7). SURF, SIVON and Google reach agreement Terms of Service Google Chrome. ⟨https://www.surf.nl/en/surf-sivon-and-google-reach-agreement-terms-of-service-google-chrome⟩.

SURF. (2023c, July 5). Privacy risks from 2021 Google Workspace for Education DPIA sufficiently resolved. Privacy risks from 2021 Google Workspace for Education DPIA sufficiently resolved.

SURF. (n.d.-a). Essential Services. Retrieved September 27, 2023, from ⟨https://www.surf.nl/files/2023-07/bijlage-list-of-essential-services.pdf⟩.

SURF. (n.d.-b). SURF is the collaborative organisation for IT in Dutch education and research. Retrieved September 27, 2023, from ⟨https://www.surf.nl/en⟩.

SURF, & SIVON. (2023, July 3). Final improvement plan Google ChromeOS and Chrome browser on Chrome devices. ⟨https://sivon.nl/wp-content/uploads/2023/07/Improvement-plan-Google-for-ChromeOS-on-managed-devices.pdf⟩.

Terra, F., Nas, S., Roosendaal, A., 2023. Inspection results Google Chrome for education. SIVON. ⟨https://sivon.nl/wp-content/uploads/2023/07/20230629-Chrome-inspection-report-v1-2-public-NEW.pdf⟩.

Thatcher, J., O'Sullivan, D., Mahmoudi, D., 2016. Data colonialism through accumulation by dispossession: new metaphors for daily data. Environ. Plan. D: Soc. Space 34 (6), 990–1006. https://doi.org/10.1177/0263775816633195.

Tietosuojavaltuutettu. (2021, December 30). Tietosuojavaltuutetun päätös käsittelyn lainmukaisuutta ja henkilötietojen siirtoa kolmansiin maihin koskevassa asiassa. Finlex. ⟨https://finlex.fi/fi/viranomaiset/tsv/2021/20211503?search%5Btype%5D=pika&search%5Bpika%5D=google⟩.

Trzaskowski, J., 2022. Data-driven business models - privacy and marketing. In: Kosta, E., Leenes, R., Kamara, I. (Eds.), Research Handbook on EU Data Protection Law. Edward Elgar, pp. 206–239.

Tuomi, I., Cachia, R., & Villar-Onrubia, D. (2023). On the Futures of Technology in Education: Emerging Trends and Policy Implications. https://doi.org/10.2760/079734.

UNESCO. (2023a). An ed-tech tragedy? Educational technologies and school closures in the time of COVID-19. ⟨https://unesdoc.unesco.org/ark:/48223/pf0000386701⟩.

UNESCO. (2023b). Global Education Monitoring Report. Technology in education: A Tool in Whose Terms? https://doi.org/10.54676/UZQV8501.

Upson, L. (2011, May 11). A new kind of computer: Chromebook. Google Official Blog. ⟨https://googleblog.blogspot.com/2011/05/new-kind-of-computer-chromebook.html?⟩+.

Vaidhyanathan, S., 2011. The Googlization of Everything (and Why We Should Worry). University of California Press.

Veliz, C., 2022. Digitization, surveillance, colonialism. Liberties 3 (1). ⟨https://libertiesjournal.com/articles/digitization-surveillance-colonialism/⟩.

VTC. (2021). Aanbeveling VTC bij de Digisprong in het onderwijs. ⟨https://overheid.vlaanderen.be/digitale-overheid/digisprong-in-het-onderwijs⟩.

VTC. (2023a). Standpunt VTC i.v.m. gebruik Google for Education door basis- en secundair onderwijs.

VTC. (2023b). Vragen VTC aan Google na Overleg met Google en na Brief aan Minister van Onderwijs. ⟨https://overheid.vlaanderen.be/sites/default/files/media/VTC/VTC_O_2023_01_vragen_aan_Google_deel_2_naVTC_def.pdf?timestamp= 1689170403⟩.

Weller, M. (2020). 25 Years of Ed Tech. ⟨10.15215/aupress/9781771993050.01⟩.

Williamson, B., 2021. Google's plans to bring AI to education make its dominance in classrooms more alarming. Fast Co. ⟨https://www.fastcompany.com/90641049/google-education-classroom-ai⟩.

Ya Shak, M.S., Mohd Tahir, M.H., Mohd Adnan, A.H., Devi Piaralal, N.S., Mohamad Shah, D.S., 2021. Google Classroom as perceived by educators: an overview. Malays. J. Soc. Sci. Humanit. (MJSSH) 6 (7), 360–369. https://doi.org/10.47405/mjssh.v6i7.867.

Zuboff, S., 2019. The age of surveillance capitalism: the fight for a human future at the new frontier of power: Vol. E-book. PublicAffairs.