Computers and Education Open 7 (2024) 100195

Contents lists available at ScienceDirect

Computers and Education Open

journal homepage: www.sciencedirect.com/journal/computers-and-education-open

# The Googlization of the classroom: Is the UK effective in protecting children's data and rights?

Sonia Livingstone [a,*], Kruakae Pothong [a], Ayça Atabey [b], Louise Hooper [c], Emma Day [d]

[a] Department of Media and Communications, London School of Economics and Political Science, Fawcett Tower, Houghton St, London, WC2A 2AE
[b] School of Law, University of Edinburgh, Old College, South Bridge, Edinburgh, EH8 9YL
[c] Garden Court Chambers, 57-60 Lincoln's Inn Fields, London, WC2A 3LJ
[d] Tech Legality, Harju maakond, Tallinn, Kesklinna linnaosa, Tornimäe tn 3 // 5 // 7, Estonia 10145

ARTICLE INFO

*Keywords:*
Google Classroom
Children's rights
Educational technology
Data protection
Commercial exploitation
Socio-legal analysis

ABSTRACT

There has been an explosion in uses of educational technology (EdTech) to support schools' teaching, learning, assessment and administration. This article asks whether UK EdTech and data protection policies protect children's rights at school. It adopts a children's rights framework to explore how EdTech impacts children's rights to education, privacy and freedom from economic exploitation, taking Google Classroom as a case study. The research methods integrate legal research, interviews with UK data protection experts and education professionals working at various levels from national to local, and a socio-technical investigation of the flow of children's data through Google Classroom. The findings show that Google Classroom undermines children's privacy and data protection, potentially infringing children's other rights. However, they also show that regulation has impacted on Google's policy and practice. Specifically, we trace how various governments' deployment of a range of legal arguments has enabled them to regulate Google's relationship with schools to improve its treatment of children's data. Although the UK government has not brought such actions, the data flow investigation shows that Google has also improved its protection of children's data in UK schools as a result of these international actions. Nonetheless, multiple problems remain, due both to Google's non-compliance with data protection regulations and schools' practices of using Google Classroom. We conclude with a blueprint for the rights-respecting treatment of children's education data that identifies needed actions for the UK Department for Education, data protection authority, and industry, to mitigate against harmful practices and better support schools.

## 1. Introduction

The UK EdTech sector is reportedly one of the fastest growing sectors attracting international investment. Estimated to be worth £10.7 billion by 2027 [1], this growth is expected to continue [2]. As a sector, EdTech is heavily driven by data. While media headlines draw attention to data breaches, cyber-attacks and other unanticipated consequences (as when the UK Department for Education made pupils' data available to gambling firms; see [3]), this article examines consequences that can reasonably be anticipated, asking whether data protection law and its application regarding personal data collected from children at school respects their rights.

Considerable efforts are underway to understand the opportunities afforded by the use of data-driven and increasingly autonomous technologies, and also the risks of widespread reliance on diverse forms of EdTech – including hardware, software and services such as school management information systems, platforms and communication tools [4]. The risks include adverse consequences of personal (and often sensitive) data entering a heavily commercial global market, often without children's, parents' or schools' knowledge or consent. It is commonly said that commercial uses of personal data are being accepted as a fair exchange for so-called 'free' EdTech, even though the educational benefit remains unclear [5,6]. But is the technology free, and is the exchange fair? Who is responsible and who benefits? These questions lead to a further question: Could regulation better protect children's privacy and their other rights, or should society accept that the

* Corresponding author at: Department of Media and Communications, London School of Economics and Political Science, Houghton Street, London WC2A 2AE, UK.
*E-mail address:* s.livingstone@lse.ac.uk (S. Livingstone).

https://doi.org/10.1016/j.caeo.2024.100195
Received 14 March 2024; Received in revised form 26 May 2024; Accepted 3 June 2024
Available online 4 June 2024

development and enforcement of regulation relating to EdTech will likely fail to keep up with the exponential growth of an industry on which schools now rely?

While vast venture capital is invested in EdTech businesses around the world [7], a few major platforms dominate the education landscape (e.g. Google Classroom, Khan Academy, Kahoot!, YouTube), recontextualizing once-public educational institutions within the corporate sphere [8]. In 2022, Google Classroom was the second most popular app in the UK, with 837,440 downloads [9]. The post-pandemic growth of Alphabet Inc. (Google's parent company) makes it the world's third largest technology company by market capitalisation [10]. This article examines the role and responsibilities of EdTech in the UK with a focus on data protection policy and practice, taking Google Classroom as a case study. With children's rights, especially to privacy, freedom from commercial exploitation and education, often marginalized in deliberations about both EdTech and data protection policy, this is a crucial moment to assess the significance of the so-called 'Googlization' of the classroom, by which we refer to the transformations – in this case relating to education - linked to the widespread adoption of Google products. In this context, Googlization has been critiqued by Kerssens, Nichols & Pangrazio [[11], p.1] as "emblematic of the growing power of private tech companies in schools across the globe, challenging education as a public good."

## 2. Research methods

Our methods examine how Google processes education data, which we define as personal data collected from children while they are learning – both at school and through their participation in school. We conducted desk research into the data governance landscape related to EdTech in the UK, including laws, policies, government strategy papers and private sector policy papers [12,13,14,15]. Then, to explore school governance and practice, between 2021 and 2022 we interviewed 47 people with various professional roles across the English school system as well as experts in data management, data protection, children's rights, standards and certification, asking them about EdTech choices, uses, data management and outcomes. Interviews were fully transcribed, anonymized and analysed using NVivo software.

Finally, we conducted a socio-technical investigation in 2022, repeated in 2024, with a small number of children and their parents by deploying a web browser plugin called Lightbeam (for Firefox) and Thunderbeam (for Chrome), to capture the data flow throughout each child's user journey through Google Classroom, one of the 'core' services in the standard (free) version of Google Workspace for Education (although, in addition, one participant had transferred to a school that used Microsoft Teams, so we explored this too). The aim of the investigation was not to sample families representatively, but to reveal the operation of the platforms through a demonstration of the data flow.

Our multidisciplinary expertise facilitated the integration of social, technical and legal methods, and these were approved by the ethics committee of our university. In combining these different methods, it proved useful to focus on one country to match national data protection regulation to both industry provision and educational practice, although we hope the UK case supports wider implications. Our reasoning for this hope rests on two international developments; the growing influence of the European General Data Protection Regulation (GDPR) and the UK's Age Appropriate Design Code (or Children's Code of the Data Protection Act) means that many countries are debating the protection of children's education data; the power of certain big tech companies means that similar challenges to protecting children's data are faced by a growing number of countries worldwide. On the other hand, as our findings show, even within Europe, the approach of countries varies considerably for reasons of national politics and culture.

## 3. A child rights analysis of Google Classroom

Google Classroom is a 'core service' within Google's Workspace for Education that can be used in conjunction with other Google Workspace for Education 'core' services such as Gmail, Docs, Sheets and 'additional' services such as Google Earth, Google Search, Google Maps and YouTube. Google [16] describes Classroom as a 'free education platform' that can boost collaboration, streamline assignments and foster communication. A teacher can manage many aspects of a class within Google Classroom: marking rubrics can be created and reused; parents and guardians can check on their child's progress; and third party products such as ClassDojo can be integrated with Google Classroom. Having created a Google account, students can access their assignments, marking schemes, documents, videos and YouTube clips (if enabled by the school) and collaborate with others, including through a chat function controlled by the teacher. Advanced (paid for) versions embed machine learning to detect plagiarism and ensure 'originality' [17]. School platform administrators can run reports to assess both child and teacher engagement and application ('apps') use (Google, [18]).

Critical analysis of digital services such as Google Classroom variously draws on theories of mediatization [19], datafication [20,21], platformization [22,23] or 'Googlization' ([11]; Vaidhyanathan, [24]). While critical scholars differ in their intellectual references and emphasis, there are common concerns with technology as opaque and complex yet infrastructural and taken for granted [25]. It is argued that the concentration of power by global tech companies and related business interests is 'reshaping the educational sector' the more they 'are deployed in relation to educational sector specific processes of personalization and datafication' (Kerssens & van Dijk [26], p. 3). Both critical scholarship and civil society advocacy are now examining the data protection practices of public education authorities and EdTech companies and their emerging forms of partnership ([27]; UNICEF, [28]). According to UNESCO's [29] *Global education monitoring report*, these partnerships give an unfair advantage to companies, overwhelm schools' competence to manage, and undermine government oversight. The resulting problems are threefold – companies' 'stranglehold on data' undermines privacy, safety, autonomy, equity and governance; adverse pedagogical impacts result as education itself is fitted to the logic and interests of 'profit-seeking technology providers'; and consumers are misled or even exploited to the point where trust is collapsing and government-led regulation, standards, accreditation and ethical procurement, as well as digital literacy and responsible business practices, are urgently called for.

These three problems are usefully framed from a human rights and child rights perspective, the latter being especially relevant to schools. The 'stranglehold on data' first and foremost infringes the right to privacy (in the UN Convention on the Rights of the Child, UNCRC, this is protected in Article 16, UN, [30]). Any adverse pedagogical impacts undermine the child's right to education (Articles 28 and 29). Finally, failures in consumer protection undermine the child's right to freedom from economic exploitation (Article 32) [31]. Additional rights relevant to the use of EdTech used at school and beyond include non-discrimination (Article 2), the best interests of the child (Article 3 (1)), evolving capacity and parent/guardian responsibility (Article 5), freedom of expression, thought and assembly (Articles 13–15), access to information (Article 17), health (Article 24), rest, leisure and play (Article 31), protection from harm (Articles 19, 34, 36) and children's knowledge of their rights (Article 42). Challengingly, a child rights approach must be holistic, both because all these rights are important and because rights are indivisible and interdependent [32].

## 4. International efforts to regulate Google's processing of children's data

The question of state responsibility is gaining prominence in public policy and legal processes, with growing disquiet about the power of the

technology sector globally and declining public trust in the EdTech sector (consider, for example, the case of Edmodo, Federal Trade Commission (FTC), [33]). There are also growing efforts to regulate Google's relationships with schools and its treatment of children's education data. In the USA in 2020, the Attorney General of New Mexico filed a complaint against Google in the State Court (United States District Court for the District of New Mexico, [34]), alleging unfair data practices when children interacted with Google's Workspace for Education products. In 2021, a settlement was reached, and Google agreed to provide schools with tools to protect children's data in compliance with applicable laws, introduce a requirement that Google deploy technical measures to recognize and refrain from commercializing data of children aged under 13, inform parents which Google services collect data from their children, and provide New Mexico schools with early access to new products as part of Google's Pilot Program [35]. To pre-empt the need for each state separately to address Google's treatment of its children's data, there have also been developments at a federal level. In 2022, the FTC [36] issued a policy statement that it was against the law to subject children to commercial surveillance as a condition of accessing educational tools or to force parents or schools to accept commercial surveillance practices.

In Europe, the GDPR has transformed the treatment of personal data, broadly defined as information relating to identified or identifiable persons, with effects felt far beyond Europe [37]. This is resulting in high-profile actions targeting Google and other companies including Microsoft whose products are widely used in schools. At stake are failures to ensure fair and transparent data practices that comply with the law, as well as deceptive and pervasive data practices, and abuse of a company's dominant market position to promote their own commercial interests. These unfair data practices are problematic from competition and data protection law perspectives. As children's right to privacy and data protection underpin their other rights in the digital environment, such data practices collectively undermine children's rights.

Already in 2019, the French data protection authority, the Commission nationale de l'informatique et des libertés (CNIL), fined Google €50 million for violating the GDPR, citing especially Google's failure to comply with GDPR's transparency and consent rules, which was later approved by the Conseil d'État [38]. CNIL [39] found that Google had carried out opaque data processing, failed to obtain valid user consent for ad personalization, and fragmented information by design (spreading it across multiple cross-referenced documents and requiring many clicks to access information). CNIL underscored the further confusion created by the plethora of services (e.g., YouTube, Google Maps and Gmail) and the lack of information about how data were combined across them. Although CNIL's decision was not specific to Google's education products, the critique clearly applies across the board, including to Google Workspace for Education and its integration with different Google services. Subsequently, CNIL [40,41] focused on its EdTech 'sandbox' projects to help the EdTech sector comply with the GDPR.

In 2021, Germany's antitrust authority, the Bundeskartellamt, took a different approach, investigating Google's market dominance and challenging Alphabet Inc. to give users sufficient choices and more control about how it uses their personal data. In 2023, the Bundeskartellamt [42,43], in cooperation with the European Commission, found that Google (Alphabet Inc.) was in the position of 'gatekeeper' and had abused that power to restrict end-users' choices over Google's processing of personal data across its services; it subsequently banned Google from applying such data processing terms in its cross-service processing. Moreover, in 2022, the Baden-Württemberg data protection authority (DPA) [44] called on schools to ensure that the software they use complies with data protection laws, leading many schools to change their software.

In the Netherlands, the Dutch DPA warned the educational sector that they would have to discontinue using Google Workspace and raised concerns about the use of Chromebooks and the Chrome browser as a result of Privacy Company's data protection impact assessment (DPIA) commissioned by the government [45], which identified Google's failure to comply with GDPR in crucial ways. Google agreed to implement organizational, contractual and technical changes to address the data protection risks identified by the Privacy Company earlier in 2021 [46].

While in France, Germany and the Netherlands the main costs have been levied on companies, schools, too, are being held responsible for Google's policies, challenging the capacity of the public sector to manage businesses' data practices. In 2020 the Swedish DPA fined the children's and education board of Östersund Municipality for failing to conduct a DPIA before using Google Workspace in schools.

In 2022, the Danish DPA prohibited the use of Google Workspace in the municipality of Helsingør and suspended data processing that involved data transfer to third countries after identifying substantial data protection risks, including transparency and inadequate international data transfer safeguards [47]. In January 2024, the Danish DPA found 53 municipalities in breach of GDPR principles (Article 5(1)), and required these municipalities to ensure their data processing, using Workspace for Education and Chromebook, complied with data protection principles by March 2024 [48]. This requirement may result in these municipalities abolishing Workspace for Education and Chromebook altogether because they cannot control Google's processing for 'derivative purposes', for example 'measuring the performance and development of new functions and services' [48].

In Iceland, too, a DPA [49] audit of primary schools' use of cloud services in several municipalities in 2022 focused on Google Workspace for Education, finding that Google cloud services were used without adequate data protection. While the DPA found Google to process students' personal data beyond instructions and agreed purposes of the local authorities, it was the municipalities that were fined a total of ISK12.8 million [49].

These international data protection decisions suggest three main points. First, Google does not appear to have carried out a sufficient DPIA of its own to confirm its compliance with the GDPR or identify existing risks. Second, the schools or municipalities as data controllers are not consistently carrying out their own basic due diligence, which would involve them carrying out a DPIA before procuring Google products for use in schools. Third, Google's market position and connected services raise questions about opaque and unfair data practices that are also become increasingly complex to navigate.

The first problem seems easier to remedy, as Google has sufficient resources to carry out a DPIA and has even implemented measures to make its data practices more transparent. The second problem is somewhat dependent on the first, since schools and municipalities require sufficient transparency from Google regarding its data practices for their own due diligence. Without this, they struggle to fulfil their legal responsibilities as data controllers. Moreover, it is unsatisfactory to expect schools to conduct their own DPIAs; it would seem more practical for all schools to receive the same data protection terms from Google, and these could be negotiated nationally rather than by each school individually. The third problem is more substantial and requires regulatory intervention, as discussed next.

## 5. Data protection challenges in practice

One in three UK 6- to 17-year-olds were asked by their school to use Google Classroom in 2021 [14]. However, for only one in five children had their school discussed what information about them was kept by the apps or websites they used at school, and even fewer had been informed about how their personal information was shared with the government or companies or their rights to correct such information or even to opt out of data collection at school. Fewer still (one in ten) thought it acceptable for the apps they used at school 'to share information about you and your classmates with other companies.' It is popularly claimed that the data protection challenges could be alleviated by teaching children digital and data literacy at school, including being informed of

their rights as data subjects. While this is undoubtedly needed [50], the foregoing socio-legal analysis suggests it would be insufficient for children to gain meaningful agency and control over their data.

The problems with Google Classroom's data processing are multiple, challenging both children and the capacity of schools to manage them. Google Workspace for Education's policies reveal that it collects and processes multiple types of data during children's use of Google Classroom. Once combined, this is sufficient to construct a full profile of each individual child including their identity, location, biometrics, preferences and abilities. This risks Google and other companies acting beyond the instructions of schools in handling data, using unfair data and design practices, for example to promote its products or inform internal product development, contra regulations about data minimization and purpose limitation [14]. Since our expert lawyers could not ascertain what data Google Classroom actually collects and how it handles these data, including when the data are shared with others (e.g., the government or future universities, employers or, indeed, data brokers or other businesses), it is no wonder that schools struggle to grasp the nature, purposes or consequences of education data processing, according to the National Education Union (P4) and a commercial DPO (P15):

> I think there are questions about Google and the use of data, and there are questions about how Google and Microsoft and Amazon become part of the infrastructure of education, and how that goes beyond just remote learning, or beyond a tool that you use at certain times or to support your practice. (P4)

> Now, if I'm using something like Google Analytics which pseudonymizes and pools data, then that's an issue, because they're doing more with the data than I want them to do… If the child is over 13, they will do some profiling. And as soon as that happens, you're meant to get consent from the parents and the child, depending on the age… By default, Google Workspace for Education doesn't have additional services to [turn] on. But schools turn on because they don't understand that. (P15)

The current regulation gives schools (as 'data controllers') the responsibility for children's data. But they receive insufficient guidance or resources to minimize risks and maximize benefits for students from using EdTech. Lacking the budget and technical/legal skills to exercise their responsibilities, schools find it near-impossible to navigate the complex technology and regulatory landscapes shaped by global data-driven businesses with competing interests. Children and parents are also unable since, even when consent is the basis of processing, their consent is likely to be invalid in a school setting where it is too difficult for a child (or parent) to refuse consent, and because the data subject is unlikely to understand what consent is given for. For example, as data controllers, especially holding often-sensitive data about children, schools should generally conduct DPIAs. However, our interviews revealed confusion and misplaced trust in both government and powerful companies such as Google:

> There's quite a bit of confusion around the need for data protection impact assessments… The classic one is generally where there's a perception amongst schools that if the local authority says it's okay, or if the government website has mentioned something, like Google Classroom, that it's being endorsed by the government … and therefore, it's all right. There's no need to do anything else. (P6, school data protection officer)

According to a former school headteacher (P2), schools tend to focus on product functionality and its suitability for teaching rather than the implication of product function and operation for data protection compliance when choosing EdTech products:

> Data protection, if I'm honest, isn't usually at the forefront of our mind when we make those kinds of decisions. Usually, it comes back to bite us on the bum at a later point and we realize that we should have thought about it. So, really, what we were thinking about was the best teaching and learning environment for our students.

According to an independent data protection officer (DPO) (P9) interviewed, schools may find comfort in doing what others do, whether or not this is effective in protecting their students' data:

> It tends to be the word of mouth, what other people are doing, what they think the local authority, or somebody might be endorsing, or in some instances, whatever the software supplier, if it's one of those, is actually telling them they're going to get the benefits from.

Even when a school DPO (P11) conducts a DPIA, they still may not understand the implications of the data being collected, how they are processed and for what purposes when using a suite of Google's services:

> The things that we use, their Gmail system, Google Drive system, Google Classroom, and I think there's something called G-Chat… Google Docs, as well, sorry. The Meet system is used… I'm not sure if that's used between students themselves, I don't know if they have permission to do that. But I don't know in terms of the other Google products outside that, how that… I don't know how we would know whether people were then going on to use other Google stuff.

As a commercial DPO (P16) who advises schools said of a particular instance when trying to understand how different Google products' privacy policies work individually, and when different Google products or services are used in conjunction with one another:

> I set her up with a Google account for the first time, just to wipe the slate clean to see how close these companies looked to complying with the [Children's] Code. And the answer is not close at all. And I read the privacy notice, and I lost the will to live. And I couldn't get to the bottom of it.

## 6. Problematic data flows through Google Classroom

Data protection risks manifest most clearly through design interfaces in Google Workspace for Education that make the boundary between the more privacy-respecting ('core') and the commercial ('additional') services provided nearly invisible and very easy to cross. We demonstrated this blurred boundary in 2022 through an investigation of the standard (free) version of Google Workspace for Education with two children aged 9 and 12 from different schools. This showed that both children had access to different ranges of 'additional' services, such as Maps, YouTube, Hangout and Search [14]. Teachers could post links within Google Classroom to resources hosted by external services, such as Vimeo.

When the 9-year-old clicked on his teacher's link to learning resources hosted by Vimeo, he was taken out of the high privacy protection of Google Classroom and exposed to 42 third party tracking services, including Google's ad service and TikTok's and Facebook's (now Meta) analytics. When the child clicked on a link to learning resources on YouTube, he was exposed to 50 additional tracking services, including TikTok, Amazon and Facebook (now Meta). The 12-year-old child from a different school had access to fewer 'additional' services; it appeared that schools applied different settings for Google Workspace for Education, whether or not they were aware of the risks of commercialization of data about children. In both cases, however, the children were exposed to a similar level of cookie surveillance. As their data enter the global data ecosystem, it may become vulnerable to data breaches, commercial exploitation and privacy risks, with long-term consequences for children's prospects, given the increasing use of automated processing in the workplace, insurance, universities and other areas. Such a situation is, arguably, the very opposite of 'privacy by design' [51], which is being increasingly called for.

In August 2021, Google agreed to implement various changes, including introducing technical controls allowing schools to block

students from accessing additional services when using Google Classroom after the Dutch DPA threatened to ban schools and universities from using Google Workspace [46], as discussed. Consequently, we revisited our investigation in the spring of 2024, aware that the international efforts to regulate Google's data processing (reviewed in Section 4) may have improved data practices. Working with an 8-year-old child from the same primary school as the 9-year-old child who joined our 2022 investigation and a 16-year-old child from a different school, we found that Google's technical improvement also applied in the UK. Both children had access to significantly fewer Google additional services compared to our findings in 2022; for example, neither child had access to YouTube, Google Maps or Google Hangouts, all of which had been available to the 9-year-old previously. As the 8-year-old attends the same primary school as the 9-year-old who participated in 2022, we could directly compare the number of 'additional' services available to the 9-year-old in 2022 and the 8-year-old in 2024 and observed this noteworthy improvement. We asked the 8-year-old's parent to verify with the school whether this change resulted from the school's platform administrator's adjustment of Workspace for Education's setting or from Google's new default setting. The parent reported that the school confirmed that the restricted access to Google's additional services was enforced by Google, resembling the technical control that Google agreed to implement after the Dutch DPA's threat to ban the product. In this case, the technical control mechanism means that students' access to services and applications that Google deems unsecure is switched *off* by default and can only be overridden by school's platform administrator. This demonstrates that regulation can significantly address the gap between what the law aims to achieve and what happens in practice.

Despite these technical improvements, our 2024 investigation showed that teachers from both schools still posted links to external (non-Google) services for students to use as part of their learning. When each child clicked on the links to these external services, they were exposed to cookie surveillance from various Google and non-Google third party services. One of the external (non-Google) learning services that the 16-year-old child accessed through the link that a teacher posted in Google Classroom exposed her to 170 third party tracking services that feed into the advertising technology infrastructure. The exception was when the 8-year-old child clicked on the link to learning material hosted on YouTube while still logged in with his school-assigned Google Classroom account; his access to YouTube was denied. According to the school's response to the 8-year-old's parent, the child's access to YouTube was denied because Google implemented another technical control restricting under-18s from hosting or creating content on social media such as YouTube, and marked all Workspace for Education accounts as under-18 by default.

It is technically feasible to block access to services with inferior privacy policies, so not blocking access to or data flow from Google Classroom to services with inferior privacy policies would facilitate the commercial exploitation of children's data through Google's affiliations and third party tracking. Interestingly, the data flow captured by Lightbeam showed that no such data appeared to flow from Microsoft Teams (when the 11-year-old participant at another secondary school clicked the links to external learning sites posted by teachers). Such a difference between data flows from these two learning platforms used in schools in England reinforces the conclusion that design matters, and that children's data could be protected within the specific learning environment even when teachers post links to external services and students click on these links. To date, Google has not provided any notification that leaving the core services means being exposed to third party data collection, for example, for the purpose of targeted advertising. Nor is it clear that the greater technical control given to the school's platform administrator is sufficient to protect children's data, given that schools' platform administrators could still activate additional services on teachers' requests and teachers can still post links to external sites. Note that although our focus here is Google, similar concerns have been raised in respect of Microsoft's 365 Education service, including shifting the responsibility for children's data to schools without making it possible for them to determine the terms on which that data is processed, opaque terms and conditions and 'secret tracking of children' [52].

While teachers posting links to learning materials hosted in Google's additional services and other external services can be seen as a behavioural or literacy problem, this same problem can be fixed with technical solutions. One option is to block access to those services with inferior privacy protection, as Google has done with the 8-year-old's attempt to access learning materials hosted on YouTube, using his school's assigned Google account. Another option, arguably better, would be to lock in all the data within Google Classroom and isolate it from third party surveillance, as is possible if the content is sandboxed within Classroom rather than shared through a clickable link that takes the user outside, and as appears to be the case for Microsoft Teams; clearly further research on improved privacy by design solutions is called for.

## 7. Rights and wrongs in EdTech policy and regulation

It is likely that a person's academic and personal history, and their achievements and failures, will have all been documented by the time they are 18 years old, and prospective universities or employers may be able to access this information at the click of a button without the person knowing or being able to correct the information held about them. Yet in post-Brexit UK, a revised data protection regime is proposed that weakens the provisions of the UK GDPR, purportedly to reduce the regulatory burden for business, arguably at the expense of children's rights. Also, in contrast to the UK, Europe appears to be moving towards increased data protections – consider, for instance, the specific provisions of the 2024 EU Artificial Intelligence Act banning AI systems designed to detect human emotions for use in education [53]. Hence, this article examined evidence that applies in the UK case to consider what arguments for policy intervention could be supported.

The promised pedagogical benefits of the 'Googlization' of the classroom are compromised by the failure adequately to regulate its data processing, although there is also evidence of improved protections for education data following international interventions. In terms of design interfaces, our 2024 Google Classroom investigation showed that the technical control measures for Google's additional service, following the Dutch investigation [54], resulted in significantly fewer of Google's additional services being available to children in their Google Classroom environment. We also observed fewer non-Google third party tracking services interacting with Google's additional services, for example, Maps and Earth, that our child participants had access to in our 2024 investigation. This highlights a positive effect of the enforcement of the EU GDPR on platform design and the resulting higher privacy protection afforded the child user by design. Nonetheless, we conclude that there is a compelling case for the UK government to better regulate the use of EdTech in schools, and for greater international attention to the multiple implications of EdTech on children's rights.

This case rests on four main arguments. First, Google and a multitude of other interconnected apps, sites and platforms are increasingly processing children's data in schools with very little oversight, and on an unprecedented scale in ways that infringe children's privacy. This lack of oversight begins with the opacity of EdTech data processing practices and privacy policies. As cited in Section 4, some of the instances in which Google has been fined by regulators for breaches of the GDPR are because they risked the privacy and security of children's data. The opaque and connected systems through which EdTech companies share data also undermine children's agency as they are not given the opportunity to engage freely with the services they use and are unaware of what happens to their data and what using Google services means for their rights [55].

Second, Google's significant power in shaping data processing in educational settings extends beyond specific breaches of data protection and competition law mentioned in regulatory decisions. The influence of

Google and other Silicon Valley companies on the pedagogical approach to teaching and learning has been documented – for example, Google is increasingly using insights gained from students to develop curriculum content and other pedagogic resources for schools. This directly impacts on the government's responsibility, as the primary duty bearer, to protect children's right to education, along with other public and civil society actors with expertise in pedagogy, learning and curriculum development.

Third, the large-scale processing of children's data in an education setting, coupled with the loss of privacy that appears insufficiently compensated by educational benefits, suggests that current prevalent practices in the EdTech sector risk the commercial exploitation of children while they learn [56,57]. Google and the wider EdTech sector are pursuing an overriding commercial imperative that relies on processing children's data at scale. The global EdTech market is expected to reach US$696.04 billion by 2028 [58]. The commercial imperative that drives the design principles of big EdTech companies should be countered with educational design principles [59] that prioritize educational value over data mining potential, particularly as AI is integrated into EdTech products [60,61]. The education market is large enough to sustain this shift in focus without making it commercially unviable.

Fourth, the specific features of EdTech design that undermine children's privacy and other rights, in conjunction with the limitations of UK data governance, also impede schools' capacity to protect the education data of their students. Governments are the primary duty bearer when it comes to protecting children's data and their broader rights affected by EdTech companies. They should both pass and implement laws and regulations such as the GDPR and the UK Age-Appropriate Design Code (Information Commissioner's Office, [62]) to effectively govern the practices of EdTech companies. As this article has shown, such regulation can be effective and beneficial for children and schools if steps are taken to require compliance.

EdTech platforms such as Google Classroom underpin vital national education infrastructure. Google's control over data processing in education, together with its opaque privacy policies, creates power imbalances among Google, governments, schools, and students. This power imbalance, along with the data protection breaches of the GDPR, aligns with broader concerns about the 'Googlization', datafication, and platformization of education. Data breaches by EdTech companies at the school or municipality level not only violate data protection law but can also negatively affect the trust that students, parents and educators place in the education system. Ceding so much power to a large American company to surveil a nation's children, and shape schools' pedagogy, fundamentally challenges a society and its children's lives and futures, even its democracy and national security.

## 8. Conclusions: Rights-respecting recommendations for EdTech policy

This article has found that regulatory enforcement by data protection authorities has proved effective in forcing change for the better at contractual, organization and technical levels. Some of these changes appear piecemeal and applied on a region-by-region basis (such as in New Mexico and the Netherlands). Others, such as changes to the general privacy policy in Europe, have been applied more widely. Of particular note in redressing the power balance between Big Tech and schools are the changes that the Dutch government negotiated restricting permitted processing purposes and shifting the burden of GDPR compliance onto the provider, Google. This makes complying with data controller responsibilities under GDPR more feasible for schools. The impact of some of these changes is transnational. The technical changes to Workspace for Education's settings are also effective when used in the UK, as demonstrated in our Google Classroom investigation. This approach can, however, lead to an international lottery for children's rights depending on their local laws and how active any relevant DPA, education authority or non-governmental organization is in enforcing compliance with the law. In the UK there has been no priority focus on children's data protection in education by the Information Commissioner's Office (ICO) owing to a lack of resources and capacity – or possibly political will. It is unclear therefore whether the contractual changes brought about in the Netherlands apply equally to British schoolchildren. The result is that in the UK children's privacy and data rights in education in comparison to our European counterparts have been somewhat overlooked. The unfolding legislative agenda could enable the UK government to cement children's rights through providing an opportunity to enshrine a requirement to conduct comprehensive risk assessments and require a code of practice for EdTech providers to adhere to in legislation. It remains to be seen whether there is appetite to do so or whether the interests of Big Tech will prevail.

Learning from international efforts to regulate Google's processing of education data, we recommend a 'blueprint' for the rights-respecting treatment of children's education data [57] as a baseline for EdTech's data processing if they are to be safely deployed in schools. We propose that schools only procure EdTech that routinely upholds the UNCRC, robustly applying the Children's Code, and complying with the UK GDPR. The UK's DPA, the ICO, should develop an education-specific checklist that enables schools to identify whether the school or the EdTech company is the data processor (a common area of confusion that blurs accountability). It is also important that the Department for Education provides guidance and standard contract terms for schools on the procurement of EdTech products to relieve them of the heavy burden of contract negotiation with multiple EdTech providers, which often involves an assessment that lies outside their area of expertise. This could be supported by a government certification scheme for EdTech, including an approved framework, and standard EdTech assessment criteria to enable schools to identify products that protect children's rights and provide clear and evidence-based pedagogical, safeguarding or administrative benefits. Finally, the UK – and other countries – need a trusted data infrastructure for research, business and government in the public's – and children's – interest. This would require defining which data should be made public and how, and developing a clear framework for data access. At present, most of the data collected are not available for public purposes, although EdTech companies get virtually unfettered access to children's data for commercial purposes. It is worth asking whether such data could become more widely available to and used by governments and independent researchers who could harness it for research and educational benefit; this should include enhancing ways that schools themselves gain data analytics or insights that genuinely inform their practice [57,63].

The strength of a children's rights perspective to EdTech governance lies in its normative authority with governments, especially in countries such as the UK that have robust human rights legislation, and a Children's Code that recognizes the primacy of the best interests of the child. In Europe, too, not only do the European Convention on Human Rights and GDPR obviously apply to children, but the European Commission [64] is also crafting its own Code of Conduct on age-appropriate design. Yet the European Commission's [65] *Digital Education Plan (2021–2027)* aims to make EdTech into 'Europe's next success story', while saying little about data protection. Beyond the UK and Europe, the UNCRC is globally the most widely ratified human rights treaty ever. The UN Committee on the Rights of the Child, which is tasked with overseeing the UNCRC's implementation, directs governments to carry out children's rights impact assessments (CRIAs) when introducing new laws and regulations, and calls on technology companies to do the same when designing and developing new products and services. The adoption of the UN Committee on the Rights of the Child's General Comment No. 25 [66] sets out a pathway for governments to realize children's rights in relation to the digital environment, and EdTech is firmly within its scope.

However, in the private sector we are witnessing something of a geopolitical war in which Europe, China and India are battling to create

their own EdTech sectors and are threatening to overtake Silicon Valley's prior dominance [67]. At the same time, the technology sector continues to push back against regulation, warning governments that they risk stifling innovation. Finding the optimal balance between EdTech innovation, especially with the growing importance of AI, and regulation to protect human and children's rights is an increasing priority [68]. It seems likely that efforts towards governance of EdTech will include the introduction of standards from IEEE, ETSI or ISO. Standards tend to be led by the private sector, and although civil society and regulators may be invited to contribute their opinions as standards are drafted, ultimately standards are a form of private sector self-regulation and existing practices related to their development leave a lot to be desired from a democratic governance perspective. The UN [69] has called on all stakeholders to 'marshal the strengths of digital technology to advance our national and international aspirations for education and lifelong learning' while mitigating the risks of the private sector's tightening grip on public education, along with the surveillance, control and commercial exploitation that so often accompany it. When it comes to the daily experience of children at school, however, these high-level discussions can seem abstract, and what matters is the David and Goliath struggle of schools to protect children's education, privacy and other rights while using 'free' EdTech products and services provided by global companies headquartered far away.

## CRediT authorship contribution statement

**Sonia Livingstone:** Writing – review & editing, Writing – original draft, Supervision, Resources, Project administration, Methodology, Investigation, Funding acquisition, Conceptualization. **Kruakae Pothong:** Writing – review & editing, Writing – original draft, Project administration, Methodology, Investigation, Conceptualization. **Ayça Atabey:** Writing – review & editing, Writing – original draft, Methodology, Investigation, Conceptualization. **Louise Hooper:** Writing – review & editing, Writing – original draft, Methodology, Investigation, Formal analysis, Conceptualization. **Emma Day:** Writing – review & editing, Writing – original draft, Investigation, Conceptualization.

## Declaration of competing interest

None.

## Acknowledgements

We are grateful to the schools, experts and families who participated in or advised on this research, and to the 5Rights Foundation for funding the Digital Futures for Children centre that supported this research.

## References

[1] Data City, The (2024). What is EdTech? UK EdTech Industry. Retrieved from https://thedatacity.com/rtics/ed-tech-rtic0010/. Accessed March 12, 2024.
[2] Department for Business & Trade (2021). EdTech. https://www.great.gov.uk/international/content/investment/sectors/edtech/.
[3] Adams, R. (2020). Department for Education's handling of pupil data ruled illegal. *The guardian*, October 7. www.theguardian.com/education/2020/oct/07/department-for-educations-handling-of-pupil-data-illegal.
[4] Department for Education. Realising the potential of technology in education. 2019. www.gov.uk/government/publications/realising-the-potential-of-technology-in-education.
[5] Meyer M, Zosh JM, McLaren C, Robb M, McCaffery H, Golinkoff RM, Hirsh-Pasek K, Radesky J. How educational are 'educational' apps for young children? App store content analysis using the Four Pillars of Learning framework. J Child Media 2021;15(4):526–48. https://doi.org/10.1080/17482798.2021.1882516.
[6] Outhwaite, L., Early, E., Herodotou, C., & Van Herwegen, J. (2023). *Can maths apps add value to learning? A systematic review*. CEPEO Working Paper Series 23–02. UCL centre for education policy and Equalising opportunities. https://econpapers.repec.org/paper/uclcepeow/23-02.htm.
[7] Davies H, Eynon R, Komljenovic J, Williamson B. Investigating the financial power brokers behind EdTech. In: Livingstone S, Pothong & K, editors. Education data futures: Critical, regulatory and practical reflections; 2022. p. 81–92. 5Rights Foundation, & Digital Futures Commission, https://educationdatafutures.digitalfuturescommission.org.uk/.
[8] Cobo C, Rivas A, editors. The new digital education policy landscape: from education systems to platforms. Routledge; 2023. https://doi.org/10.4324/9781003373018.
[9] Statista (2024a). Leading educational mobile applications in the United Kingdom in 2022. Retrieved from www.statista.com/statistics/1266710/uk-most-downloaded-education-apps/. Accessed 12 March 2024.
[10] Statista (2024b). Leading tech companies worldwide 2024, by market capitalization. Retrieved from www.statista.com/statistics/1350976/leading-tech-companies-worldwide-by-market-cap/. Accessed March 12, 2024.
[11] Kerssens N, Nichols TP, Pangrazio L. Googlization(s) of education: intermediary work brokering platform dependence in three national school systems. Learn Media Technol 2023:1–14. https://doi.org/10.1080/17439884.2023.2258339.
[12] Day, E. (2021a). *Governance of data for children's learning in UK state schools*. Digital Futures Commission. https://eprints.lse.ac.uk/119734/.
[13] Day E, Pothong K, Atabey A, Livingstone S. Who controls children's education data? A socio-legal analysis of the UK governance regimes for schools and EdTech. Learn Media Technol 2022:1–15. https://doi.org/10.1080/17439884.2022.2152838.
[14] Hooper L, Livingstone S, Pothong K. Problems with data governance in UK schools: The cases of Google Classroom and ClassDojo. Digital Futures Commission 2022. https://eprints.lse.ac.uk/119736/.
[15] Turner S, Pothong K, Livingstone S. Education data reality: the challenges for schools in managing children's education data. Digital Futures Commission 2022. http://eprints.lse.ac.uk/119731/.
[16] Google (n.d.-a). Google Classroom is the main address of Education, Training, Study! https://sites.google.com/view/classroom-workspace/.
[17] Google (2022). Privacy & terms - list of services & service specific additional terms. https://policies.google.com/terms/service-specific.
[18] Google (n.d.-b) Google Workspace Admin Help - Monitor usage and security with reports. https://support.google.com/a/answer/6000239?hl=en.
[19] Rawolle, S., & Lingard, B. (2014). Mediatization and education: a sociological account. In K. Lundby (Ed.), The Handbook of Mediatization (pp. 595–616). De Gruyter Mouton. https://doi.org/10.1515/9783110272215.595.
[20] Jarke J, Breiter A. Editorial: the datafication of education. Learn Media Technol 2019;44(1):1–6. https://doi.org/10.1080/17439884.2019.1573833.
[21] Pangrazio L, Selwyn N, Cumbo B. A patchwork of platforms: Mapping data infrastructures in schools. Learn Media Technol 2023;48(1):65–80. https://doi.org/10.1080/17439884.2022.2035395.
[22] Helmond A. The platformization of the web: Making web data platform ready. Social Media + Society 2015;1(2). https://journals.sagepub.com/doi/10.1177/2056305115603080.
[23] Nichols TP, Dixon-Román E. Platform governance and education policy: Power and politics in emerging Edtech ecologies. Educ Eval Policy Anal 2024. https://doi.org/10.3102/01623737231202469.
[24] Vaidhyanathan S. The Googlization of everything (And why we should worry). University of California Press; 2012.
[25] Plantin J-C, Lagoze C, Edwards PN, Sandvig C. Infrastructure studies meet platform studies in the age of Google and Facebook. New Media Soc 2018;20(1):293–310. https://doi.org/10.1177/1461444816661553.
[26] Kerssens N, van Dijck J. Transgressing local, national, global spheres: The blackboxed dynamics of platformization and infrastructuralization of primary education. Inf Commun Soc 2023:1–17. https://doi.org/10.1080/1369118X.2023.2257293.
[27] Human Rights Watch (2022). Governments harm children's rights in online learning. News, May 25. www.hrw.org/news/2022/05/25/governments-harm-children-rights-online-learning.
[28] UNICEF (2021). Policy guidance on AI for children - Version 2.0 | Recommendations for building AI policies and systems that uphold child rights. https://www.unicef.org/globalinsight/reports/policy-guidance-ai-children.
[29] UNESCO. (2023). *Global education monitoring report 2023: Technology in education: A tool on whose terms?* https://doi.org/10.54676/UZQV8501.
[30] UN (1989) Convention on the Rights of the Child (UNCRC). Treaty Series, vol. 1577, p. 3. www.refworld.org/docid/3ae6b38f0.html.
[31] van der Hof S, Lievens E, Milkaite I, Verdoodt V, Hannema T, Liefaard T. The child's right to protection against economic exploitation in the digital world. The Int J Children's Rights 2020;28(4):833–59. https://doi.org/10.1163/15718182-28040003.
[32] UN Human Rights Office of the High Commissioner (2023). What are human rights? www.ohchr.org/en/what-are-human-rights.
[33] FTC (2023). Edmodo, LLC, U.S. v. (May). www.ftc.gov/legal-library/browse/cases-proceedings/202-3129-edmodo-llc-us-v.
[34] United States District Court for the District of New Mexico. (2020). State of New Mexico, ex rel., Hector Balderas, Attorney General of the State of New Mexico v. Google LLC.
[35] New Mexico Department of Justice (2021). Attorney General Hector Balderas announces landmark settlements with Google over children's online privacy. Press release, December 13. Retrieved from https://nmdoj.gov/press-release/attorney-general-hector-balderas-announces-landmark-settlements-with-google-over-childrens-online-privacy/. Accessed March 12, 2024.
[36] FTC (Federal Trade Commission) (2022). *Policy statement of the Federal Trade Commission on education technology and the children's online privacy protection act*. May 19. www.ftc.gov/legal-library/browse/policy-statement-federal-trade-commission-education-technology-childrens-online-privacy-protection.

[37] Ryngaert, C., & Taylor, M. (2020). The GDPR as global data protection regulation? *AJIL Unbound*, 114, 5–9. https://doi.org/10.1017/aju.2019.80.
[38] Conseil d'État (2020). RGPD: Le Conseil d'État rejette le recours dirigé contre la sanction de 50 millions d'euros infligée à Google par la CNIL. June 19. www.conseil-etat.fr/actualites/rgpd-le-conseil-d-etat-rejette-le-recours-dirige-contre-la-sanction-de-50-millions-d-euros-infligee-a-google-par-la-cnil.
[39] CNIL (Commission nationale de l'informatique et des libertés). (2019). Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC. www.cnil.fr/sites/cnil/files/atoms/files/san-2019-001.pdf.
[40] CNIL (2022). EdTech 'sandbox': The CNIL supports 10 innovative projects. Retrieved from www.cnil.fr/en/edtech-sandbox-cnil-supports-10-innovative-projects/. Accessed March 12, 2024.
[41] CNIL (2023). Digital health and EdTech: The CNIL publishes the results of its first 'sandboxes. Retrieved from www.cnil.fr/en/digital-health-and-edtech-cnil-publishes-results-its-first-sandboxes/. Accessed March 12, 2024.
[42] Bundeskartellamt (2023a). Bundeskartellamt gives users of Google services better control over their data. Retrieved from www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/05_10_2023_Google_Data.html/. Accessed March 12, 2024.
[43] Bundeskartellamt (2023b). Decision pursuant to Section 19a(2) sentence 4 in conjunction with section 32b(1) GWB. retrieved from www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2023/B7-70-21.pdf?_blob=publicationFile&v=2/. Accessed March 12, 2024.
[44] Baden-Württemberg Data Protection Authority. (2022). Schulen auf dem Weg zu datenschutzfreundlichen Lösungen. https://www.baden-wuerttemberg.datenschutz.de/schulen-auf-dem-weg-zu-datenschutzfreundlichen-loesungen/.
[45] Nas, S., & Terra, F. (2021a). *DPIA on the use of Google G Suite (enterprise) for education*. privacy company. retrieved from www.surf.nl/files/2021-06/updated-g-suite-for-education-dpia-12-march-2021.pdf. Accessed March 11, 2024.
[46] Nas, S., & Terra, F. (2021b). Update DPIA report Google Workspace for Education. Privacy Company, August 2. Retrieved from www.surf.nl/files/2021-08/update-dpia-report-2-august-2021.pdf. Accessed March 11, 2024.
[47] Datatilsynet (2022, July 14). Datatilsynet nedlægger behandlingsforbud i Chromebook-sag. https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/jul/datatilsynet-nedlaegger-behandlingsforbud-i-chromebook-sag.
[48] OneTrust (2024, January 31). Denmark: Datatilsynet issues injunction on municipalities in google workspace case. DataGuidance. https://www.dataguidance.com/news/denmark-datatilsynet-issues-injunction-municipalities.
[49] Personuvernd (2023). Úttekt á notkun Reykjanesbæjar á skýjalausn Google í grunnskólastarfi. https://www.personuvernd.is/urlausnir/uttekt-a-notkun-reykjanesbaejar-a-skyjalausn-google-i-grunnskolastarfi.
[50] Pangrazio, L., & Sefton-Green, J. (Eds.). (2022). *Learning to live with datafication: educational case studies and initiatives from across the world*. Routledge.
[51] Cavoukian, A. (2011). *Privacy by Design: The 7 foundational principles. Implementation and mapping of fair information practices*. https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.
[52] NOYB (2024, June 4) Microsoft violates children's privacy – but blames your local school. https://noyb.eu/en/microsoft-violates-childrens-privacy-blames-your-local-school.
[53] European Parliament (2023). Artificial Intelligence Act. Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 –2021/0106(COD)). www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf.
[54] Nas, S., & Terra, F. (2023). *Verification report google remediation measures, workspace for education for SURF and SIVON*. privacy company, July 23. Retrieved from www.surf.nl/files/2023-07/20230724-clean-workspace-for-education.pdf. Accessed March 11, 2024.
[55] Day, E. (2021b). Why all data governance needs to consider children's rights. Berkman Klein Center Collection. https://medium.com/berkman-klein-center/why-all-data-governance-needs-to-consider-childrens-rights-8b218a825a08.
[56] Atabey, A., Livingstone, S., & Pothong, K. (2023) When are commercial practices exploitative? Ensuring child rights prevail in a digital world. Digital Futures Commission (20 Feb 2023) http://eprints.lse.ac.uk/id/eprint/119542.
[57] Kidron B, Pothong K, Hooper L, Livingstone S, Atabey A, Turner S. A Blueprint for Education Data: Realising children's best interests in digitised education. Digital Futures Commission 2023. https://eprints.lse.ac.uk/119737/.
[58] Arizton (2023). EdTech market - Global outlook & forecast 2023-2028 2028. Retrieved from www.arizton.com/market-reports/edtech-market/. Accessed March 12, 2024.
[59] Kucirkova N. The promise and pitfalls of personalised learning with new EdTechLivingstone S, Pothong K, editors. The promise and pitfalls of personalised learning with new EdTech. Education data futures: critical, regulatory and practical reflections. (221-230) Digital Futures Commission 2022. https://educationdatafutures.digitalfuturescommission.org.uk/.
[60] Kerssens N, van Dijck J. Governed by Edtech? Valuing pedagogical autonomy in a platform society. Harvard Educ Rev 2022;92(2):284–303. https://doi.org/10.17763/1943-5045-92.2.284.
[61] Veale, M. (2022). Schools must resist big EdTech – but it won't be easy. In S. Livingstone, & K. Pothong (Eds.), Education data futures: Critical, regulatory and practical reflections. (67-78) Digital Futures Commission. https://educationdatafutures.digitalfuturescommission.org.uk/.
[62] Information Commissioner's Office (2020). *Age appropriate design: a code of practice for online services*. Retrieved from https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/ Accessed March 11, 2024.
[63] Selwyn, N., Pangrazio, L., & Cumbo, B. (2021). Attending to data: Exploring the use of attendance data within the datafied school. Res Educ, 109, 1, 72–89. https://doi.org/10.1177/0034523720984200.
[64] European Commission (2023a). Special group on the EU Code of conduct on age-appropriate design. Shaping Europe's digital future. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/group-age-appropriate-design/. Accessed March 12, 2024.
[65] European Commission (2023b). Making EdTech into Europe's next success story. Eur Education Area. News, May 10. https://education.ec.europa.eu/node/2464.
[66] UN Human Rights Office of the High Commissioner (2021). General Comment No. 25 (2021) on children's rights in relation to the digital environment (CRC/C/GC/25). Retrieved from www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx. Accessed March 11, 2024.
[67] Lynch, M. (2020). How geopolitics are influencing the Edtech market. The Tech Edvocate, April 22. www.thetechedvocate.org/how-geopolitics-are-influencing-the-edtech-market/.
[68] Dignum, V. (2023). Future-proofing AI: regulation for innovation, human rights and societal progress. Foundation for European Progressive Studies, June 15. https://feps-europe.eu/future-proofing-ai-regulation-for-innovation-human-rights-and-societal-progress/.
[69] UN (United Nations) (n.d.). *Assuring and improving quality public digital learning for all*. www.un.org/en/transforming-education-summit/digital-learning-all.