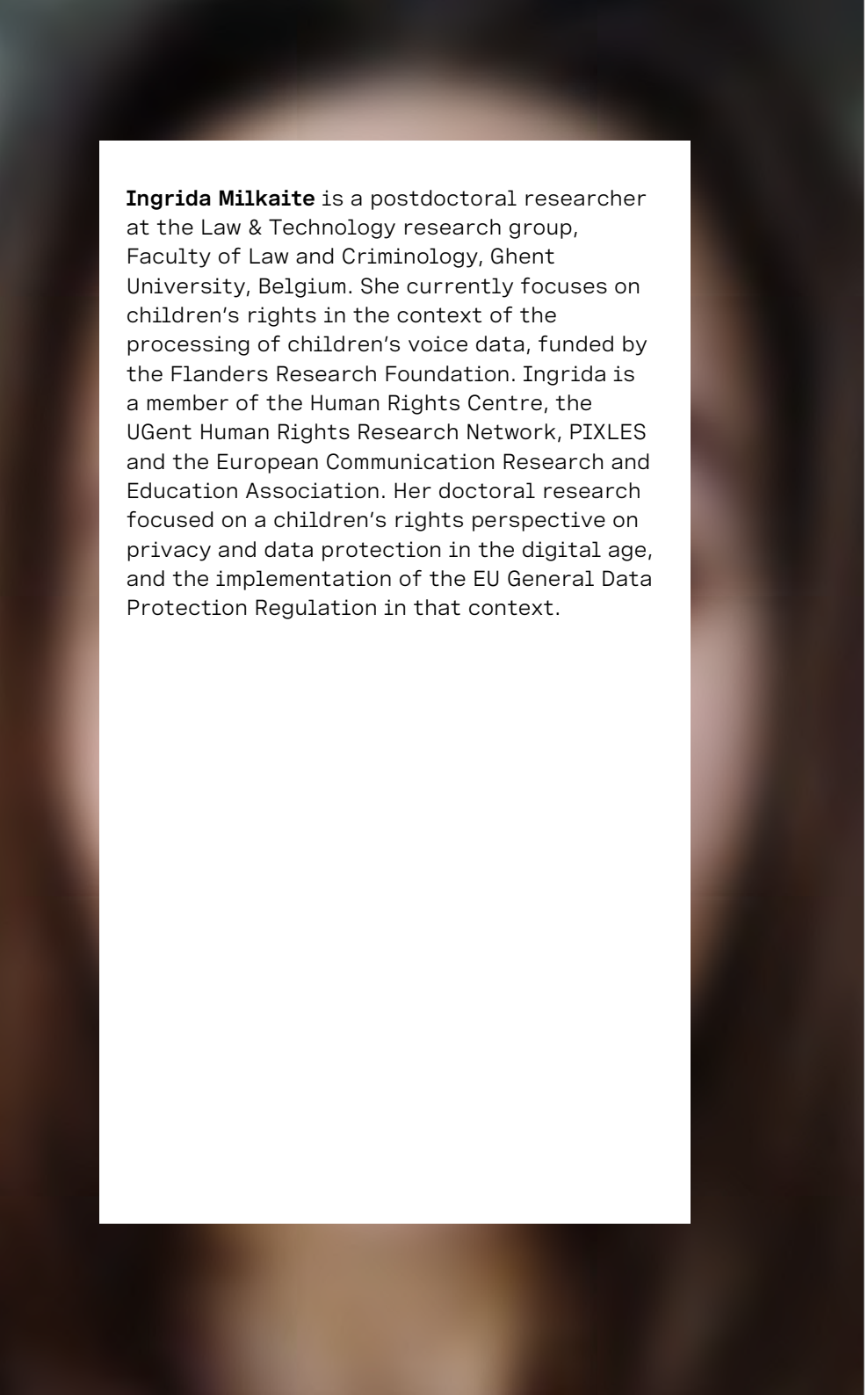

Ingrida Milkaite is a postdoctoral researcher at the Law & Technology research group, Faculty of Law and Criminology, Ghent University, Belgium. She currently focuses on children's rights in the context of the processing of children's voice data, funded by the Flanders Research Foundation. Ingrida is a member of the Human Rights Centre, the UGent Human Rights Research Network, PIXLES and the European Communication Research and Education Association. Her doctoral research focused on a children's rights perspective on privacy and data protection in the digital age, and the implementation of the EU General Data Protection Regulation in that context.

An international perspective on data protection for children's education data

Ingrida Milkaite, Ghent University

Today's children are 'datafied' as soon as they are born or undergo their first medical scans in utero (Lupton & Williamson, 2017). Their families further develop their digital traces, resulting in 80% of children younger than two having a digital footprint in Western countries (UN General Assembly, 2021, para. 86). As they grow older, their digital records continue to expand exponentially - in the home, social and school environments.

In recent years (and especially during the COVID-19 pandemic), we have witnessed a growing reliance on educational technologies, or EdTech. Many believe that the use of EdTech can benefit teachers and students (UN Committee on the Rights of the Child, 2021), but it is crucial to remember that the use of most digital technologies is intrinsically linked with the processing† of children's personal data by the various actors providing them.

In the words of the UN Special Rapporteur on the right to privacy, children's 'immersion in the ever-expanding range of

† 'Processing' can be defined as 'any operation or set of operations performed on personal data, such as but not only the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure or destruction of, or the carrying out of logical and/or arithmetical operations on such data' (CoE, 2020a, p. 7).

digital technologies produces an ongoing stream of data, collected and enhanced by artificial intelligence, machine-learning applications and facial and speech recognition technologies' (UN General Assembly, 2021). This context calls for the vigorous implementation of data protection and children's rights law to guide the development and use of EdTech.

Processing children's personal data in the educational environment

In November 2020, the Council of Europe (CoE) adopted specific guidelines on children's data protection in an education setting (CoE, 2020a). It specifically called for recognition of the 'breadth of personal data that may be processed, its wide uses including in support of learning and non-learning aims, for administration, behavioural management and teaching purposes, its sensitivity, and the lifelong risks to privacy that may arise from processing both non-digitised and digitised records in an educational setting' (CoE, 2020a, p. 5). This is important as children's education data is now not only provided by children themselves, their parents, caregivers and teachers, but is also deduced from 'data that is created as a by-product of user engagement or data that is inferred (for instance on the basis of profiling)' (CoE, 2020a, p. 11).

The processing of children's personal data in the educational setting† used to focus on 'routine' monitoring of the security and physical movement of the pupils (Lupton & Williamson, 2017). Now, in addition to relying on cameras to keep an eye on students and (unwelcome) visitors to schools, biometric tracking technologies are also increasingly employed, for example, facial or voice recognition, and iris, fingerprint or palm vein scanning (Alba, 2020; Leaton Gray, 2018; Steeves et al., 2018). The Information Commissioner's Office (ICO) – the UK data protection authority (DPA) – recently decided to intervene and investigate concerns about the use of facial recognition technology on pupils queuing for lunch in the canteens of nine schools (Weale, 2021). The use of such technologies in schools has already led to fines for unlawful processing of children's personal data in Sweden, and has been banned altogether in France (IAPP, 2019; Lee, 2019).

Today's education data landscape is ever-expanding and has generally been shifting towards the routine collection and analysis of children's increasingly sensitive personal data (Lupton & Williamson, 2017; Taylor, 2013). This change is associated with processes such as data or learning analytics,† e-learning platforms,‡ behaviour monitoring programmes and ever-growing educational databases. Consequently, children's learning data may now include 'thinking characteristics, learning trajectory, engagement score, response times, pages read, and videos viewed' (UN General Assembly, 2021, para. 107).

In addition to monitoring students' academic progress, some use 'emotional learning analytics' that can 'make extensive use of psychometrics, sentiment analysis and natural language processing [and] employ other data sources such as face cams, video, eye tracking, skin temperature and conductivity to enable the automatic detection, assessment, analysis and prediction of the emotional state of learners' (Lupton & Williamson, 2017, p. 785). Such 'learning analytics' constitute one of the most significant forms of child tracking in the contemporary educational setting since these technologies 'mine data about learners as they go about educational tasks and activities in real time and provide automated predictions of future progress that can then be used as the basis for intervention and pre-emption' (Lupton & Williamson, 2017, p. 785).

Another related issue concerns children's profiling in the educational environment. Profiling can be understood as:

> any form of automated processing of personal...

† Here, 'educational setting' or 'educational context' refers to schools attended by children under the age of 18. However, the discussed issues, concerns and recommendations are also very relevant and, in many cases, applicable in the context of other educational institutions, such as universities and colleges.

† 'Data analytics' 'refers to personal data used in the computational technologies that analyse large amounts of data to uncover hidden patterns, trends and correlations, and refers to the whole data management lifecycle of collecting, organising and analysing data to discover patterns, to infer situations or states, to predict and to understand behaviours', while 'learning analytics' 'can be described as the measurement, collection, analysis and reporting of data about learners and their contexts, for the purposes of understanding and optimising learning and the environments in which it occurs' (CoE, 2020a, pp. 6, 7).

‡ The term 'e-learning' 'may broadly include learning with the support of information and communication technologies (ICT), especially for delivery or accessing of content, distance learning or web-based learning (including tools used in online and offline modes)' (CoE, 2020a, p. 7).

> ... data including use of machine learning systems consisting of the use of personal or non-personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. (CoE, 2020a, p. 7)

While profiling may be used for evaluating and personalising education, it is also associated with data - that children can hardly challenge - being hardcoded into their profiles and potentially following them throughout their educational and professional paths for the rest of their lives (Livingstone et al., 2021). Given that a profile 'refers to a set of characteristics attributed to an individual, characterising a category of individuals or intended to be applied to an individual' (CoE, 2020a, p. 7), profiling children may lead to 'sorting them into boxes'. Due to an algorithm's categorisation of a specific child, children may be provided with limited information and education opportunities, negatively affecting their rights to non-discrimination, development, identity, education and information. According to the UN Special Rapporteur on the right to privacy, profiling children 'limits their potential self-development in childhood, adolescence and possibly adulthood, as behavioural predictions and nudging techniques can predetermine options and choices' (UN General Assembly, 2021, para. 92). Therefore, EdTech needs 'to be assessed against children's rights and best interests' (ibid).

While the educational environment is associated with the processing of children's personal data on an increasingly large scale and over long periods of time (CoE, 2020a, p. 17), the exact impact of data-fuelled EdTech learning on children's education, development and future lives is neither clear, nor foreseeable. Few voices are questioning the actual benefits these technologies may bring for children since many of the products and services seem very appealing as they promise enhanced learning and personalised education for individual children. However, current automated processes, decisions and predictions on children's educational trajectories are very opaque and difficult to understand for children, parents, caregivers, teachers and schools. Despite their appeal and anticipated potential, the exact learning outcomes for children using EdTech are currently contentious and unproven (Defend Digital Me, 2020; Livingstone et al., 2021).

'Datafication' of children for commercial goals

Complex revenue models operate behind the various fun activities accessible to children online - including through EdTech - 'creating value for companies by feeding children's data into algorithms and self-learning models to profile them and offer personalised advertising or by nudging children to buy or try to win in-app items' (van der Hof et al., 2020, p. 833). Notably, the national DPAs in the UK and Ireland have recently expressed serious doubts as to whether commercial interests can be reconciled with the best interests of the child in the digital environment (ICO, 2020; Irish Data Protection Commission, 2020).

The selection of different EdTech is also influenced by the fact that some are offered to schools for free (with such software now being referred to as 'freeware') (CoE, 2020a, p. 3). In this context, schools may struggle to make informed risk-benefit decisions. Financial considerations may outweigh potential privacy and data protection issues, even though it has already been shown that many EdTech applications collect excessive amounts of children's personal data, including their device identifiers and location data, which, in many cases, may then be shared with third parties and advertisers (Kelly, 2019; Ng, 2020; UN General Assembly, 2021, para. 108; Wodinsky, 2021). As children's data increasingly 'fuel the business of the digital world' (UN General Assembly 2021, para. 90; see also Zuboff, 2019), the question as to whether these processes actually benefit children and their best interests remains contentious.

Meaningful implementation of data protection and children's rights law

Any digital service that processes children's personal data needs to comply with data protection law requirements. These include service providers' accountability, the requirement for

the lawful ground for data processing, such as meaningful consent or public interest task, compliance with the principles of fairness, transparency, purpose limitation, data minimisation, data protection by default and by design. The EU also requires specific protection of children's personal data and imposes stricter requirements for such processing (e.g., Recital 38 of the General Data Protection Regulation, GDPR).

Specific protection for children includes the requirement for data-processing information to be tailored particularly to them (Article 12); special vigilance regarding child profiling (Recital 71); a reinforced right to be forgotten (Recital 65); the child's right not to be subject to automated individual decision-making (Article 22) and the requirement for data protection impact assessments (DPIAs) when new technologies are used and the data processing is likely to result in a high risk to children's rights.

The principles of service providers' accountability, fairness and the requirement for specific protection of children's personal data (Articles 24 and 5(1)(a) GDPR, Recital 38) closely relate to the requirement to consider children's best interests as a primary consideration in any action affecting them. This stems from Article 3 of the UN Convention on the Rights of the Child (UNCRC). Whereas its provisions are primarily directed at States, the UN Committee on the Rights of the Child has emphasised that the Convention's provisions should also be respected by private businesses as the business sector affects children's rights in the provision of digital services (UN Committee on the Rights of the Child, 2013, 2021).

A precautionary approach

Despite the promises of personalisation, enhanced learning and improved education results, the actual positive impact of EdTech on children's learning remains unclear (Defend Digital Me, 2020, p. 45; Livingstone et al., 2021). Recent research indicates a clear need for evidence-based and child-centric risk assessment of technologies used by children, including EdTech (UN General Assembly, 2021, para. 82). Therefore, a crucial point in this contribution relates to the fact that many – if not most – of the anticipated benefits that EdTech may bring are not yet proven, and may instead lead to negative consequences for children's rights and future lives.

Generally, the precautionary principle 'compels society to act cautiously if there are certain – but not necessarily absolute – scientific indications of a potential danger and if not acting upon these indications could inflict harm', and it has 'traditionally been accepted that it is justified to err on the side of caution when it comes to the protection of vulnerable beings against potential harm' (Lievens, 2010, pp. 38, 42; 2021). This principle has been endorsed by both the CoE and UN (CoE, 2018; UN Committee on the Rights of the Child, 2021). The CoE specifically noted the need for a 'precautionary approach and a strengthened protection towards sensitive, special categories of data, including genetic and biometric data, and ethnic origin, or relating to sexual orientation, or offences, recognising children's additional vulnerability' (CoE, 2020a, p. 8). It also explicitly relied on the precautionary principle with regard to processing children's biometric data in the educational setting (CoE, 2020a, p. 20).†

It is currently very difficult to assess and predict the impact that extensive processing of children's (sensitive) data, profiling, personalisation, learning analytics and behavioural monitoring programmes developed by commercial actors will have on children('s rights) in the long term. Aside from a potential substantial impact on children's rights to privacy and data protection, there may be direct or collateral impact on their rights to development, identity, non-discrimination, freedom of thought, expression and association, as well as the right to protection from commercial exploitation. Bearing in mind that doubts exist as to whether data-processing practices in the educational environment are in some ways harmful to children, it would be in line with the best interests of the child to conduct fundamental, empirical and longitudinal evidence-based research on the matter first (Lievens, 2020, 2021).

The basic idea underpinning the precautionary principle relates to the adoption of risk mitigation measures in situations of inconclusive or incomplete evidence in terms of risks

† Specifically, '… processing characteristics about voice, eye movement, and gait; social emotional and mental health, and mood; and reactions to neurostimulation, for the purposes of influencing or monitoring a child's behaviour should be done on the basis of a precautionary principle and treated as biometric data' (CoE, 2020a, p. 20).

(Gellert, 2016). One such practical measure is a data protection impact assessment (DPIA), which is in certain cases required by the GDPR (Article 35). Many national DPAs have classified the processing of children's personal data for certain purposes as high-risk activities, and some specifically refer to children's data processing in the educational environment as high risk (Milkaite, 2021). Whether specifically required or not, carrying out DPIAs provides an opportunity for EdTech providers to take children's rights and best interests into account when their educational data is processed.

In addition to concerns surrounding children's data and privacy, it is also crucial to acknowledge that 'it is not only the child's right to data protection that is affected when it comes to education and digital technologies and that the right to privacy and data protection are enabling rights to the protection of further rights of the child' (CoE, 2020a, p. 11). Consequently, the CoE has also noted service providers' responsibility to conduct DPIAs, and stressed that these 'should have regard for the specific impact on children's rights and should demonstrate that the outcomes of algorithmic applications are in the best interests of the child and ensure that a child's development is not unduly influenced in opaque ways' (CoE, 2020a, p. 19; UN Committee on the Rights of the Child, 2013, paras 77-81).

In order to evaluate and implement children's best interests meaningfully, DPIAs should draw from children's rights impact assessments (CRIAs) so that EdTech providers can assess and take various rights of the child into account when they consider processing children's education data.† In line with a children's rights-based perspective and best interests, both CRIAs and DPIAs should be undertaken every time EdTech processes children's data. In light of children's right to be heard, these assessments should also actively involve children, and draw from their opinions and views associated with the EdTech they may be using every day (CoE, 2020a, p. 16).

† Whereas the 'rationale for conducting CRIA was originally formulated for States as the primary duty-bearers in public-decision making, … the same rationale is now also being extended to businesses.' The same can be said about human rights impact assessments and human rights due diligence requirements. These tools were also initially addressed at states but are now also directed at industry actors (Mukherjee et al., 2021, pp. 6, 11, 12). See also: CoE (2020); UN Committee on the Rights of the Child (2013).

Recommendations for national DPAs

The CoE has made a powerful acknowledgement that children 'cannot see or understand how large their digital footprint has become or how far it travels to thousands of third parties across or beyond the education landscape, throughout their lifetime' (CoE, 2020a, p. 4). At the same time, it also stresses that 'children's agency is vital and they must be better informed of how their own personal data are collected and processed' (CoE, 2020a, p. 4). In this regard it is essential to note that a consensus exists that 'children [and their parents and caregivers] cannot be expected to understand a very complex online environment and to take on its responsibilities alone' (CoE, 2020a, p. 4). In my view, however, the issue of extensive processing of children's (sensitive) data in the educational environment cannot be fully and meaningfully addressed through calls for child empowerment, resilience and data literacy.†

To a large extent, the limit of child empowerment is rooted in a power imbalance between children, parents and caregivers, schools and service providers.‡ States as the primary duty bearer for realising children's rights have obligations to enable children, parents and schools to exercise their agency. Therefore, policymakers and national DPAs have the responsibility to 'develop evidence-based standards and guidance for schools and other bodies responsible for procuring and using educational technologies and materials to ensure these deliver proven educational benefits and uphold the full range of children's rights' (CoE, 2020a, p. 6). Most importantly, States are responsible for holding service providers to account.

The accountability of EdTech providers in terms of the existing data protection and children's rights law requirements

† This statement is made without prejudice to the requirements that 'States should ensure that easily accessible, meaningful, child-friendly and age-appropriate information about privacy tools, settings and remedies is made available to children. Children and/or their parents or carers or legal representatives should be informed by a data controller how their personal data is being processed. This should include information for instance on how data is collected, stored, used and disclosed, on their rights to access their data, to rectify or erase this data or object to its processing, and how to exercise their rights' (CoE, 2018, para. 33).

‡ The increase in the use of EdTech 'amplified existing power imbalances between education technology companies and children' (UN General Assembly, 2021, para. 106), and 'most children and parents do not have the capacity to challenge educational technology companies' privacy arrangements or to refuse to provide data, as education is compulsory' (UN General Assembly, 2021, para. 107)

should be better ensured and enforced by DPAs. In addition to adopting specific guidance, codes of (best) practice and certification schemes on children's educational data, they should also require that EdTech providers adopt, rely on and publicly disclose their CRIAs and DPIAs (CoE, 2020a, p. 16; 2020b, para. 5.3), which should be developed in direct cooperation and consultation with children. Any such guidance and codes provided by DPAs should also be regularly reviewed in line with the rapidly evolving digital developments in the EdTech sector, and also be based on consultations with children.

Generally, it appears that 'there is a mindset of collecting [all possible data] now and thinking about what to do with it later' (Livingstone et al., 2021, p. 8). Such an attitude to children's education data is contrary to the principles of data minimisation and purpose limitation, as well as the best interests of the child and their right to privacy, as the processing of data must not involve more data than necessary to achieve the legitimate purpose for which it is collected. In this context, and in line with the precautionary principle, policymakers and DPAs should 'require the refusal of certain systems when their deployment leads to high risks of irreversible damage or when, due to their opacity, human control and oversight become impractical' (CoE, 2020b, p. 6). Indeed, national DPAs should be eager to enforce the existing data protection law requirements and consider the potential of imposing certain limits on children's education data processing.

The CoE has proposed a number of such limitations - for instance, that biometric data should not be routinely processed in educational settings, and that children's educational data 'should not be processed to serve or target behavioural advertisements' (CoE, 2020a, paras 7.7.1, 8.3.7). Both the CoE and the UN Committee on the Rights of the Child advocate for the prohibition of profiling with regard to children, unless scientific evidence shows that this can be done in the best interests of children and that appropriate safeguards are provided (CoE, 2020a, para. 7.6.2; UN Committee on the Rights of the Child, 2021). The CoE also maintains that using children's education data for data analytics and product development

cannot be considered 'legitimate compatible use for further processing [of children's education data] that override a child's best interests or rights' (CoE, 2020a, para. 7.1.11). In the same vein, EdTech providers should not be allowed to 'give away children's personal data collected in the course of their education, for others to monetise, or reprocess it for the purposes of selling anonymised or de-identified data, for example to data brokers' (CoE, 2020a, para. 7.1.12). In line with the purpose limitation and data minimisation principles, as well as children's best interests, only the minimum necessary amount of identifying data should be retained at the time when children leave education (CoE, 2020a, para. 7.4.1).

Finally, aside from implementing these and other recommendations for processing children's education data, national DPAs should also ensure that the rights and values of the UN Convention on the Rights of the Child (concerning in particular non-discrimination, development and privacy) clearly underpin their policies and decisions as 'children do not lose their human rights by virtue of passing through the school gates' (UN Committee on the Rights of the Child, 2001, para. 8). We need to ensure that this is also the case when children use EdTech.

Alba, D. (2020). Facial recognition moves into a new front: Schools. *The New York Times*, 6 February

CoE (Council of Europe). (2018). *Recommendation CM/Rec(2018)7 of the Committee of Ministers to Member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment*

CoE. (2020a). *Children's data protection in an education setting*. Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal data, Convention 108. Guidelines

CoE. (2020b). *Recommendation CM/Rec(2020)1 of the Committee of Ministers to Member States on the human rights impacts of algorithmic systems*

defenddigitalme. (2020). *The state of data 2020*

Gellert, R. (2016). We have always managed risks in data protection law: Understanding the similarities and differences between the rights-based and the risk-based approaches to data protection. *European Data Protection Law Review*, 2(4), 481-492

Kelly, H. (2019). School apps track students from classroom to bathroom, and parents are struggling to keep up. *The Washington Post*, 29 October

IAPP (International Association of Privacy Professionals). (2019). CNIL bans high schools' facial-recognition programs. 29 October

ICO (Information Commissioner's Office). (2020). *Age appropriate design: A code of practice for online services (the final version)*. 2 September

Irish Data Protection Commission. (2020). *Children front and centre. Fundamentals for a child-oriented approach to data processing (the fundamentals)*. Draft version for public consultation

Leaton Gray, S. (2018). Biometrics in schools. In J. Deakin, E. Taylor, & A. Kupchik (Eds.), *The Palgrave international handbook of school discipline, surveillance, and social control* (pp. 405-424). Springer International Publishing

Lee, D. (2019). School's facial recognition checks lead to fine. BBC News, 27 August

Lievens, E. (2010). *Protecting children in the digital era: The use of alternative regulatory instruments*. Brill Nijhoff

Lievens, E. (2020). *The rights of the child in the digital environment: From empowerment to re-responsibilisation*. In Essay collection on Freedom, Security, Privacy and the Future of Childhood in the Digital World, 17 June. 5Rights Foundation

Lievens, E. (2021). Growing up with digital technologies: How the precautionary principle might contribute to addressing potential serious harm to children's rights. *Nordic Journal of Human Rights*, 39(2), 128-145

Livingstone, S., Atabey, A., & Pothong, K. (2021). *Addressing the problems and realising the benefits of processing children's education data. Report on an expert roundtable*. Digital Futures Commission, 5Rights Foundation

Lupton, D., & Williamson, B. (2017). The datafied child: The dataveillance of children and implications for their rights. *New Media & Society*, *19*(5), 780-794

Milkaite, I. (2021). *A children's rights perspective on privacy and data protection in the digital age: A critical and forward-looking analysis of the EU General Data Protection Regulation and its implementation with respect to children and youth*. Dissertation, Ghent University

Mukherjee, S., Pothong, K., & Livingstone, S. (2021). *Child rights impact assessment. A tool to realise children's rights in the digital environment*. 5Rights Foundation, Digital Futures Commission

Ng, A. (2020). Education apps are sending your location data and personal info to advertisers. CNET, 1 September

Steeves, V., Regan, P., & Shade, L. R. (2018). Digital surveillance in the networked classroom. In J. Deakin, E. Taylor, & A. Kupchik (Eds.), *The Palgrave international handbook of school discipline, surveillance, and social control* (pp. 445-466). Springer International Publishing

Taylor, E. (2013). Surveillance schools: A new era in education. In E. Taylor (Ed.), *Surveillance schools: Security, discipline and control in contemporary education* (pp. 15-39). Palgrave Macmillan UK

UN Committee on the Rights of the Child. (2001). *General Comment No. 1 (2001) Article 29 (1): The aims of education* (CRC/GC/2001/1a

UN Committee on the Rights of the Child. (2013). *General Comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights*

UN Committee on the Rights of the Child. (2021). *General Comment No. 25 (2021) on children's rights in relation to the digital environment*

UN General Assembly. (2021) *Artificial intelligence and privacy, and children's privacy. Report of the Special Rapporteur on the right to privacy*. Joseph A. Cannataci. A/HRC/46/37. Human Rights Council

van der Hof, S., Lievens, E., Milkaite, I., Verdoodt, V., Hannema, T., & Liefaard, T. (2020). The child's right to protection against economic exploitation in the digital world. *The International Journal of Children's Rights*, 28(4), 833-859

Weale, S. (2021). ICO to step in after schools use facial recognition to speed up lunch queue. *The Guardian*, 18 October

Wodinsky, S. (2021). 60% of school apps are sharing your kids' data with third parties. *Gizmodo*, 5 April

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs