



Universidade do Estado do Rio de Janeiro

Faculdade de Direito

KU Leuven

Faculty of Law and Criminology



Elora Raad Fernandes

**Navigating the digital classroom:
Analyzing risks to children's data protection in educational
technology**

Rio de Janeiro
2024

Elora Raad Fernandes

**Navigating the digital classroom:
Analyzing risks to children's data protection in educational technology**

Dissertation presented in partial fulfillment of the requirements for the joint degree of Doctor of Law by the Graduate Program in Law at the State University of Rio de Janeiro (Universidade do Estado do Rio de Janeiro - UERJ), Concentration Area: Legal Thought and Social Relations, and by the Catholic University of Leuven (KU Leuven)

Supervisors:

Prof. Dr. Carlos Affonso Pereira de Souza

Prof. Dr. Peggy Valcke

Prof. Dr. Sergio Marcos Carvalho de Ávila Negri

Rio de Janeiro

2024

CATALOGAÇÃO NA FONTE
UERJ/REDE SIRIUS/BIBLIOTECA CCS/C

F363 Fernandes, Elora Raad.

Navigating the digital classroom: Analyzing risks to children's data protection in educational technology / Elora Raad Fernandes. - 2024. 348f.

Orientador: Prof. Dr. Carlos Affonso Pereira de Souza.

Orientador: Prof. Dr. Peggy Valcke Prof.

Coorientador: Prof. Dr. Sergio Marcos Carvalho de Ávila Negri.

Dissertação (Mestrado). Universidade do Estado do Rio de Janeiro, Faculdade de Direito. KU Leuven, Faculty of Law and Criminology.

1. Tecnologia educacional - Teses. 2. Proteção de Dados - Teses. 3. Crianças e adolescentes - Teses. I. Souza, Carlos Affonso Pereira de. II. Valcke, Peggy. III. Negri, Sergio Marcos Carvalho de Ávila. IV. Universidade do Estado do Rio de Janeiro. Faculdade de Direito. V. KU Leuven. Faculty of Law and Criminology. VI. Título. 37:343.45

Bibliotecária: Ana Clara Brandão CRB7/6346

Autorizo, apenas para fins acadêmicos e científicos, a reprodução total ou parcial desta tese, desde que citada a fonte.

Assinatura

Data

Elora Raad Fernandes

**Navigating the digital classroom:
Analyzing risks to children's data protection in educational technology**

Dissertation presented in partial fulfillment of the requirements for the joint degree of Doctor of Law by the Graduate Program in Law at the State University of Rio de Janeiro (Universidade do Estado do Rio de Janeiro - UERJ), Concentration Area: Legal Thought and Social Relations, and by the Catholic University of Leuven (KU Leuven)

Approved on 27 February, 2024.

Examination Committee:

Prof. Dr. Carlos Affonso Pereira de Souza (Supervisor)
Faculdade de Direito – UERJ

Prof. Dr. Els Kindt
Faculty of Law, Universiteit Leiden

Prof. Dr. Peggy Valcke (Supervisor)
Faculty of Law and Criminology – KU Leuven

Prof. Dr. Eva Lievens
Faculty of Law and Criminology – Ghent University

Prof. Dr. Sergio Marcos Carvalho de Ávila Negri (Co-Supervisor)
Faculdade de Direito – Universidade Federal de Juiz de Fora

Prof. Dr. Daniel Bucar
Faculdade de Direito – UERJ

Prof. Dr. Ilse Samoy (Chair)
Faculty of Law and Criminology – KU Leuven

Prof. Dr. Laura Drechsler
Faculty of Law and Criminology – KU Leuven

ACKNOWLEDGEMENTS

First and foremost, I thank God for all the resources entrusted to me in this existence to undertake the tasks we have set for myself. Firm in my belief that nothing is left to chance, I am immensely grateful for all the opportunities and people I have encountered on the path that has led me here. I view this as an immense responsibility to seize every moment of life and to offer my best to others, and I hope I have completed part of that mission.

I express my profound gratitude to my advisors and co-advisor, Prof. Dr. Carlos Affonso Souza, Prof. Dr. Peggy Valcke, and Prof. Dr. Sergio Negri, for their trust in me and my work, for all the support during the development of this thesis, and for their critical insights that significantly improved the research. I extend my thanks to the professors on my Supervisory Committee and Examination Committee—Prof. Dr. Daniel Bucar, Prof. Dr. Els Kindt, Prof. Dr. Eva Lievens, Prof. Dr. Laura Drechsler, and Prof. Dr. Ilse Samoy—who dedicated time and effort to read, criticize, and discuss this thesis to ensure its best version was defended. A significant work, even if small, is only possible by standing on the shoulders of giants. The Elora who began her academic journey in 2017, and came into contact with the important work of various brilliant scholars within the realm of data protection and beyond, never imagined that she would have the honor of having several of them on her jury.

I thank the State University of Rio de Janeiro (UERJ) and the Coordination for the Improvement of Higher Education Personnel (Capes) for making this PhD possible, as well as KU Leuven, which warmly welcomed me for a joint PhD experience. More specifically, I thank my fellow colleagues at UERJ, who were so important in the beginning of this journey and inspired me to become a more dedicated and serious scholar. I also thank the KU Leuven Centre for IT and IP Law (CiTiP), represented by its Head of Unit Jan de Bruyne, and all my current and former colleagues for providing a stimulating and challenging environment that helps me grow as a researcher and human being every day.

I express my heartfelt gratitude to my family, who always believed in me and my potential with unwavering support, sparing no effort to encourage me even in the face of the most unlikely ideas, and offering me all their love so I could persevere even in the toughest times. In particular, I thank my mother, father, and sister who have been daily by my side, even from across an ocean. My thanks also go to friends and colleagues I have had the pleasure of meeting along the way on various occasions, who brought company, joy and purpose to my journey.

I thank Alan, who makes my existence immensely happier every day. Thank you for providing me with a light and meaningful relationship, for being my best friend and my anchor, believing in me even in moments when I am most certain I will fail. The finalization of this thesis would definitely not have been possible without all your support, essential feedback, and encouragement.

It is also important to acknowledge my gratitude to those who were present throughout my professional career, providing opportunities for me to gain experience beyond academia. In particular, I thank all former colleagues at ARTICLE 19 Brazil and South America, represented by Denise Dora, Laura Tresca and Paulo José Lara, who believed in my potential and gave me the chance to work in an environment aligned with my ideals. I also thank former colleagues at the European Data Protection Supervisor (EDPS), represented by Brendan Van Alsenoy and Anna Buchta, who provided me with one of the most enriching experiences of my career, altering its trajectory and leading me to consider Belgium my second home.

Finally, I express my gratitude to all those who, even invisibly, enabled these experiences through the funding of public and quality education, both in Brazil and in Belgium. I recognize the privilege and responsibility of completing a PhD, especially at a university in the Global South, where many people still struggle to have their most basic human rights realized.

ABSTRACT

FERNANDES, Elora Raad. **Navigating the Digital Classroom**: Analyzing risks to children's data protection in educational technology. 2024. 348 f. Thesis – PhD in Law, Universidade do Estado do Rio de Janeiro; KU Leuven, Rio de Janeiro, 2024.

Educational technology (edtech) has vast potential to transform education by improving access, engagement, and equity, especially in the wake of the COVID-19 pandemic. The full realization of these benefits is, however, still a distant prospect. The changes observed thus far seem incremental and uneven, with their impact being heavily contingent on the socio-economic context of the communities where they are implemented, as well as the preparedness and willingness of educators to adopt them. Moreover, edtech can still yield concerning side effects, particularly in relation to children's rights to privacy and to the protection of personal data. Given that children dedicate a significant portion of their time to educational activities, the detailed digital dossiers created about them can potentially affect their academic performance, university admissions, job prospects, and access to essential public services. Using the theory of data colonialism as a normative framework, the thesis aimed to map the challenges that edtech presents to children's rights to privacy and to the protection of personal data, and understand the extent to which the current legal framework in Brazil and the European Union (EU) address them. Examining children's experiences with edtech and its impact on their development and learning processes is crucial for understanding the future of individual and collective autonomy, as well as the transformation of citizenship and the trajectory of our society. The thesis starts by delving into the history of edtech, the interplay between edtech implementation and ongoing education discussions, and the theory of data colonialism as the theoretical framework (Part I). Part II describes and analyzes how the EU and the Brazilian legal framework regulate children's privacy and data protection, focusing on Convention on the Rights of the Child, the GDPR and the LGPD. Part III focuses on mapping horizontal challenges related to children's privacy and data protection arising from the implementation of Artificial Intelligence (AI) in education and specific challenges encountered in some edtech, based on a typology developed in Part I. Part III also includes a study on Google Workspace for Education as a framework to understand the specificities in the implementation of other edtech. Overall, it confirms the research hypothesis that the current operation of AI systems in education and the widespread business model based on data commodification pose challenges to children's best interests that have not yet been addressed in the current data protection frameworks in Europe and Brazil.

Keywords: educational technology (edtech); children's data protection; data Colonialism; Google Workspace for Education.

RESUMO

FERNANDES, Elora Raad. **Navegando pela sala digital**: uma análise de riscos à proteção de dados de crianças e adolescentes nas tecnologias educacionais. 2024. 348 f. Tese (Doutorado) – Doutorado em Direito, Universidade do Estado do Rio de Janeiro; KU Leuven, Rio de Janeiro, 2024.

Tecnologias educacionais (edtech) possuem um vasto potencial para transformar a educação, melhorando o acesso, o engajamento e a igualdade, especialmente após a pandemia de COVID-19. A realização plena desses benefícios, no entanto, ainda é uma perspectiva distante. As mudanças observadas até agora parecem incrementais e desiguais, com seu impacto sendo fortemente condicionado pelo contexto socioeconômico das comunidades onde são implementadas, bem como pela preparação e disposição dos educadores em adotá-las. Além disso, edtech ainda podem gerar efeitos colaterais preocupantes, especialmente em relação aos direitos de crianças à privacidade e à proteção de dados pessoais. Dado que estas dedicam uma parte significativa de seu tempo a atividades educacionais, os detalhados dossiês digitais criados sobre elas podem afetar potencialmente seu desempenho acadêmico, admissões universitárias, perspectivas de emprego e acesso a serviços públicos essenciais. Usando a teoria do colonialismo de dados como marco teórico, a tese teve como objetivo mapear os desafios que as edtech apresentam para os direitos das crianças à privacidade e à proteção de dados pessoais, e entender até que ponto o atual marco normativo no Brasil e na União Europeia (UE) os endereçam. Examinar as experiências das crianças com edtechs e o impacto em seu desenvolvimento e processos de aprendizagem é crucial para entender o futuro da autonomia individual e coletiva, bem como a transformação da cidadania e a trajetória de nossa sociedade. A tese começa explorando a história das edtechs, a interação entre a implementação de edtechs e as discussões educacionais em andamento, e a teoria do colonialismo de dados como marco teórico (Parte I). A Parte II descreve e analisa como o marco regulatório da UE e do Brasil regulamentam a privacidade e a proteção de dados de crianças, com foco na Convenção sobre os Direitos da Criança, no GDPR e na LGPD. A Parte III concentra-se em mapear desafios horizontais relacionados à privacidade e à proteção de dados das crianças decorrentes da implementação de Inteligência Artificial (IA) na educação e desafios que edtechs específicas apresentam, com base em uma tipologia desenvolvida na Parte I. A Parte III também inclui um estudo sobre o Google Workspace for Education como um exemplo para entender as especificidades na implementação de outras edtechs. Ao final, confirma-se a hipótese de pesquisa de que o atual funcionamento de sistemas de IA na educação e o modelo de negócios baseado na comodificação de dados pessoais apresentam desafios para o melhor interesse das crianças que ainda não foram endereçados nas atuais leis de proteção de dados na Europa e no Brasil.

Palavras-chave: tecnologias educacionais; proteção de dados de crianças e adolescentes; colonialismo de dados; Google Workspace for Education.

SAMENVATTING

FERNANDES, Elora Raad. **Navigeren door de digitale klas: Analyseren van risico's voor de gegevensbescherming van kinderen in onderwijstechnologie.** 2024. 348 blz. Thesis (doctoraat) - Doctoraat in de Rechten, Universidade do Estado do Rio de Janeiro; KU Leuven, Rio de Janeiro, 2024.

Educatieve technologie (edtech) heeft enorm potentieel om het onderwijs te transformeren door de toegang, betrokkenheid en gelijkheid te verbeteren, vooral in het licht van de COVID-19-pandemie. De volledige realisatie van deze voordelen lijkt echter nog steeds ver weg. De tot nu toe waargenomen veranderingen lijken geleidelijk en ongelijk, waarbij hun impact sterk afhankelijk is van de sociaal-economische context van de gemeenschappen waar ze worden geïmplementeerd, evenals de bereidheid en bereidheid van opvoeders om ze aan te nemen. Bovendien kan edtech nog steeds zorgwekkende bijwerkingen hebben, met name met betrekking tot de rechten van kinderen op privacy en de bescherming van persoonsgegevens. Aangezien kinderen een aanzienlijk deel van hun tijd besteden aan educatieve activiteiten, kunnen de gedetailleerde digitale dossiers die over hen zijn aangemaakt potentieel van invloed zijn op hun academische prestaties, universitaire toelatingen, carrièremogelijkheden en toegang tot essentiële openbare diensten. Met behulp van de theorie van datakolonialisme als normatief kader, had de scriptie tot doel de uitdagingen te in kaart te brengen die edtech presenteert voor de rechten van kinderen op privacy en de bescherming van persoonsgegevens, en te begrijpen in hoeverre het huidige wettelijke kader in Brazilië en de Europese Unie (EU) deze aanpakken. Het onderzoeken van de ervaringen van kinderen met edtech en de impact ervan op hun ontwikkeling en leerprocessen is cruciaal voor het begrijpen van de toekomst van individuele en collectieve autonomie, evenals de transformatie van burgerschap en de koers van onze samenleving. De scriptie begint met een diepgaande verkenning van de geschiedenis van edtech, de interactie tussen de implementatie van edtech en lopende onderwijsdiscussies, en de theorie van datakolonialisme als theoretisch kader (Deel I). Deel II beschrijft en analyseert hoe het wettelijk kader van de EU en Brazilië de privacy van kinderen en de gegevensbescherming reguleren, met de nadruk op het Verdrag inzake de Rechten van het Kind, de GDPR en de LGPD. Deel III richt zich op het in kaart brengen van horizontale uitdagingen met betrekking tot de privacy van kinderen en gegevensbescherming die voortkomen uit de implementatie van Kunstmatige Intelligentie (AI) in het onderwijs, evenals specifieke uitdagingen die zich voordoen bij sommige edtech, gebaseerd op een typologie ontwikkeld in Deel I. Deel III omvat ook een studie naar Google Workspace for Education als een kader om de specificiteiten in de implementatie van andere edtech te begrijpen. Over het algemeen bevestigt het de onderzoekshypothese dat de huidige werking van AI-systemen in het onderwijs en het wijdverspreide bedrijfsmodel gebaseerd op gegevenscommodificatie uitdagingen vormen voor het beste belang van kinderen die nog niet zijn aangepakt in de huidige kaders voor gegevensbescherming in Europa en Brazilië.

Trefwoorden: educatieve technologie (edtech); bescherming van gegevens van kinderen; datokolonialisme; Google Workspace for Education.

LIST OF FIGURES

Figure 1 - Edtech typology	49
Figure 2 - The CO:RE classification of online risks to children	83
Figure 3 - AI Act risk-based approach - pyramid of risks	136
Figure 4 - Global heatmap measuring how well each country's spoken languages are represented by the composition of natural language datasets.....	177
Figure 5 - Six levels of automation of personalized learning.....	193
Figure 6 - Google Workspace for Education's core and additional services	214

LIST OF TABLES

Table 1 - Examples of EdTech “products”, with % Global Market share (2019).....	51
Table 2 - Franglen’s Admissions Algorithm	178
Table 3 - Inferring pupils’ attention through brain waves.....	180
Table 4 - Ofqual’s algorithms for evaluating students’ performance.....	188
Table 5 – Gaggle and its impacts on privacy and mental health	205

LIST OF ACRONYMS AND ABBREVIATIONS

ABNT	<i>Associação Brasileira de Normas Técnicas</i> [Brazilian National Standards Organization]
AEPD	<i>Agencia Española de Protección de Datos</i> [Spanish Data Protection Authority]
ADHD	Attention deficit hyperactivity disorder
AI	Artificial Intelligence
AIA	Artificial Intelligence Act
AIED	Artificial Intelligence in Education
ANPD	<i>Autoridade Nacional de Proteção de Dados</i> [Brazilian Nacional Data Protection Authority]
AP	<i>Autoriteit Persoonsgegevens</i> [Dutch Personal Data Authority]
APA	American Psychological Association
API	Application Programming Interface
AR	Augmented reality
Art.	Article
ATS	Applicant Tracking Systems
BIK+	European Strategy for a better internet for kids
BNCC	<i>Base Nacional Curricular Comum</i> [Brazilian National Common Curricular Base]
CAI	Computer-Aided Instruction
CBL	Computer-based Learning
CBT	Computer-based Training
CC	<i>Código Civil</i> [Brazilian Civil Code]
CDC	<i>Código de Defesa do Consumidor</i> [Brazilian Consumer Protection Code]
CD-ROM	Compact Disc-Read Only Memory
CFR	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CLR	Comprehensive Learner Records

CLV	Customer lifetime value
CNE	<i>Conselho Nacional de Educação</i> [Brazilian National Education Council]
CNIL	<i>Commission Nationale de l'Informatique et des Libertés</i> [French Data Protection Authority]
CoE	Council of Europe
Consed	<i>Conselho Nacional de Secretários da Educação</i> [Brazilian National Council of State Secretaries of Education]
COPPA	Children's Online Privacy Protection Rule (USA)
COREPER	EU Committee of Permanent Representatives
CRC	Convention on the Rights of the Child
CRFB	<i>Constituição da República Federativa do Brasil</i> [Brazilian Federal Constitution]
CRIA	Child-rights Impact Assessment
DA	Data Act
DBTS	Dialogue-Based Tutoring System
DDBM	Data-driven business model
DDDM	Data-driven decision-making
DEAP	Digital Education Action Plan
DGA	Data Governance Act
DINUM	<i>Directeur Interministériel du Numérique</i> [French Interministerial Director of Digital Affairs]
DPA	Data Protection Authority
DPC	Data Protection Commission [Irish Data Protection Authority]
DPD	Data Protection Directive
DPIA	Data Protection Impact Assessment
DSA	Digital Services Act
DSK	<i>Datenschutzkonferenz</i> [German Data Protection Conference]
DSSC	Data Spaces Support Centre
DTIA	Data Transfer Impact Assessment
EBIA	<i>Estratégia Brasileira de Inteligência Artificial</i> [Brazilian Artificial Intelligence Strategy]

ECA	<i>Estatuto da Criança e do Adolescente</i> [Brazilian Child's and Adolescent's Statute]
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EDSC	European Digital Skills Certificate
Edtech	Education technology
EEA	European Economic Area
EU	European Union
EWS	Early warning systems
FTC	Federal Trade Commission
FERPA	Family Educational Rights and Privacy Act (USA)
GDPR	General Data Protection Regulation
GEGs	Google Educator Groups
GPAI	General-purpose Artificial Intelligence
HDI	Human Development Index
IBM	International Business Machines Corporation
IBO	International Baccalaureate Organization
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICO	Information Commissioner's Office [UK's Data Protection Authority]
ICT	Information and Communication Technologies
IMEI	International Mobile Equipment Identity
IMY	<i>Integritetsskyddsmyndigheten</i> [Swedish Authority for Privacy Protection]
ISS	Information Society Services
ITS	Intelligent Tutoring Systems
KPI	Key Performance Indicator
LAI	<i>Lei de Acesso à Informação</i> [Brazilian Access to Public Information Law]

LDB	<i>Lei de Diretrizes e Bases da Educação Nacional</i> [Brazilian National Education Guidelines and Bases Law]
LGBTIQA+	Lesbian, gay, bisexual, transgender, intersex, queer/questioning, asexual
LGPD	<i>Lei Geral de Proteção de Dados Pessoais</i> [Brazilian General Data Protection Law]
LMS	Learning Management Systems
MAC	Media Access Control
MCI	<i>Marco Civil da Internet</i> [Brazilian Internet Bill of Rights]
MCTI	<i>Ministério da Ciência, Tecnologia e Inovação</i> [Ministry of Science, Technology, and Innovation]
MEC	<i>Ministério da Educação</i> [Brazilian Ministry of Education]
ML	Machine learning
MOOC	Massive Open Online Course
MP	<i>Medida Provisória</i> [Provisional Measure]
MR	Mixed reality
MS	Member States
MTST	<i>Movimento dos Trabalhadores sem Teto</i> [Brazilian Homeless Worker Movement]
NLP	Natural language processing
NGEU	Next Generation EU
NPRM	Notice of Proposed Rulemaking
OECD	Organization for Economic Cooperation and Development
Ofqual	Office of Qualifications and Examinations Regulation (UK)
PC	Personal Computer
PLE	Personal Learning Environment
PNE	<i>Plano Nacional de Educação</i> [Brazilian National Education Plan]
PNED	<i>Política Nacional de Educação Digital</i> [Brazilian Policy on Digital Education]
SDGs	Sustainable Development Goals
SDK	Software development kit
SIVON	Dutch cooperative of school boards in primary and secondary education

STF	<i>Supremo Tribunal Federal</i> [Brazilian Supreme Federal Court]
SURF	The collaborative organization for IT in Dutch education and research
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
ToS	Terms of Service
UDHR	Universal Declaration of Human Rights
UIS	UNESCO Institute for Statistics
UK	United Kingdom
UN	United Nations
UNDP	United Nations Development Program
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNICEF	United Nations Children Fund
USA	United States of America
VLE	Virtual Learning Environments
VR	Virtual reality
VTC	<i>Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens</i> [Flemish Supervisory Commission for the processing of personal data]
WP29	Article 29 Data Protection Working Party
XR	Extended Reality

TABLE OF CONTENTS

	INTRODUCTION	20
	Research question and methodology	24
a)	<u>Relevance.....</u>	24
b)	<u>Research question(s).....</u>	26
c)	<u>Hypothesis</u>	26
d)	<u>Scope of the research</u>	27
e)	<u>Methodological approach and thesis structure</u>	28
I	SETTING THE SCENE.....	32
1	The use of technology in education	33
1.1	<u>A brief history of edtech</u>	35
1.2	<u>Edtech typology</u>	47
	<u>Interim conclusion</u>	51
2	Exploring the interplay between edtech and longstanding discussions in education.....	53
2.1	<u>Public and private values in education</u>	53
2.1.1	The role of philanthropy in education	56
2.2	<u>The “learnification” of education</u>	58
2.3	<u>Learning, calculation and efficiency.....</u>	60
2.4	<u>Platform learning</u>	62
	<u>Interim conclusion</u>	64
3	Data Colonialism as a theoretical and normative framework.....	65
3.1	<u>The concept of data colonialism</u>	65
3.2	<u>Main components of data colonialism.....</u>	67
3.3	<u>Colonizing agents</u>	69
3.4	<u>Data Commodification.....</u>	70
3.5	<u>Data colonialism and its incursion into autonomy</u>	71
	<u>Interim conclusion</u>	73
II	LEGAL FRAMEWORK ON CHILDREN’S PRIVACY AND DATA PROTECTION	75
4	Why children need special privacy and data protection rights.....	76
4.1	<u>Why do children’s data require special treatment?.....</u>	77
4.1.1	Childhood as an extra layer of vulnerability.....	77

4.1.2	A proportionally larger digital footprint	79
4.2	<u>Privacy and data protection as a cross-cutting dimension of risks to children's online presence</u>	81
4.3	<u>The importance of privacy and data protection for children's development and learning</u>	85
	<u>Interim conclusion</u>	87
5	The CRC in the digital environment	89
5.1	<u>The right to non-discrimination</u>	91
5.2	<u>The right to have the child's best interests taken as a primary consideration</u>	92
5.3	<u>The right to be given appropriate direction and guidance in a manner consistent with the evolving capacities of the child</u>	95
5.4	<u>The right to have their views given due weight in accordance with their age and maturity</u>	96
5.5	<u>The right to privacy</u>	98
5.6	<u>The right to education</u>	100
5.7	<u>The right to protection against economic exploitation</u>	104
	<u>Interim conclusion</u>	106
6	EU's relevant legal and policy frameworks	107
6.1	<u>The General Data Protection Regulation (GDPR)</u>	109
6.1.1	General Principles.....	109
6.1.2	Roles and responsibilities	112
6.1.3	Article 8, GDPR.....	114
6.1.3.1	ISS	114
6.1.3.2	Offering directly to a child	116
6.1.3.3	Age for consent.....	116
6.1.3.4	Consent as an appropriate legal basis for processing children's data.....	118
6.1.4	Other legal bases for processing children's data	121
6.1.4.1	Contractual necessity	122
6.1.4.2	Compliance with a legal obligation	123
6.1.4.3	Vital interest.....	124
6.1.4.4	Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	124
6.1.4.5	Legitimate interests.....	125
6.1.5	Analysis of selected data subjects' rights	127
6.1.5.1	Transparency obligations and the right of access	127

6.1.5.2	Rectification and erasure	128
6.1.5.3	Right to data portability	129
6.1.5.4	Right to object.....	130
6.1.5.5	Automated individual decision-making.....	132
6.1.6	Data Protection Impact Assessment (DPIA)	134
6.2	<u>AI Act</u>	135
6.3	<u>EU policy on digital education</u>	141
7	Brazil's relevant legal frameworks	145
7.1	<u>The Brazilian General Data Protection Law (LGPD)</u>	146
7.1.1	General Principles for Data Processing	146
7.1.2	Art. 14, LGPD.....	147
7.1.2.1	Children's consent and applicable legal bases for processing children's data	148
7.1.2.2	Transparency obligations.....	153
7.1.2.3	Purpose limitation and data minimization requirements	154
7.1.3	Other legal bases for processing children's data	155
7.1.4	Data subjects' rights	157
7.1.5	DPIA	158
7.2	<u>The right to education</u>	159
7.3	<u>The Brazilian Artificial Intelligence Bill</u>	160
7.4	<u>Brazilian policy on digital education</u>	162
III	CHALLENGES INTRODUCED BY EDTECH TO CHILDREN'S RIGHTS TO PRIVACY AND TO THE PROTECTION OF PERSONAL DATA.....	166
8	Mapping the challenges introduced by edtech	168
8.1	<u>Datafication</u>	168
8.1.1	Reduction and abstraction.....	169
8.1.2	Data collection for AI systems operation	171
8.2	<u>Data Generation</u>	172
8.2.1	Bias	176
8.2.2	The challenge of controlling inferences based on personal data	178
8.3	<u>Decision-making</u>	180
8.3.1	Profiling	181
8.3.2	Predictions	184
8.3.2.1	Crystallization of the past	184
8.3.2.2	Unfalsifiability and preemptive intervention.....	186

8.3.2.3	Performativity	187
8.3.3	Human mis-interpretation and mis-use of data.....	190
8.3.4	Personalized learning.....	194
8.3.4.1	Technologies for Personalized Learning	196
8.3.4.2	Lack of robust evidence of their effectiveness	198
8.3.4.3	Limits to personalization	199
8.3.4.4	Content filtering.....	200
8.3.5	Student monitoring technologies	201
8.3.5.1	Behavior Monitoring	202
8.3.5.2	e-Proctoring	205
8.3.6	Learning Analytics and further use of data.....	206
	<u>Interim conclusion</u>	210
9	Google Workspace for Education	212
9.1	<u>What is Google Workspace for Education</u>	212
9.2	<u>The main features of Google Workspace for Education</u>	215
9.3	<u>The role of Google Workspace for Education within Google’s business model</u>	217
	<u>Interim conclusion</u>	223
10	The use of Google Workspace for Education in the European Union and in Brazil	225
10.1	<u>Belgium</u>	226
10.2	<u>Denmark</u>	229
10.3	<u>Finland</u>	233
10.4	<u>France</u>	235
10.5	<u>Germany</u>	236
10.6	<u>Netherlands</u>	238
10.7	<u>Norway</u>	241
10.8	<u>Spain</u>	243
10.9	<u>Sweden</u>	245
10.10	<u>Brazil</u>	246
10.10.1	The formalization of the relationship between Google and the schools.....	248
10.10.2	Privacy and data protection issues.....	251
10.10.2.1	Roles and responsibilities	252
10.10.2.2	Purposes for processing personal data	253
10.10.2.3	Lawful Bases	254

10.10.2.4	Transparency obligations.....	255
	<u>Interim Conclusion</u>	258
11	Analysis	260
11.1	<u>Tensions between the GDPR, LGPD and Google Workspace for Education</u>	260
11.1.1	Roles and responsibilities	260
11.1.2	Purposes for processing personal data	262
11.1.3	Lawful Bases	264
11.1.4	Transparency obligations.....	266
11.1.5	DPIA and risk assessment	267
11.1.6	Data Transfers.....	269
11.2	<u>Appropriation of resources through the lack of compliance with the data protection framework</u>	270
11.3	<u>Unequal data relations and global distribution of the benefits of resource appropriation</u>	271
11.4	<u>Digital sovereignty</u>	272
11.4.1	The concept of digital sovereignty	273
11.4.2	Data colonialism actors and digital sovereignty	275
11.4.3	A broader notion of digital sovereignty	277
	<u>Interim Conclusion</u>	279
	CONCLUDING REMARKS	280
	Recommendations and indications for future research	289
	REFERENCES	294

INTRODUCTION

1. Education is the cornerstone of any contemporary society. More than an isolated element used as a tool for acquiring knowledge and skills, education plays a multiplying role in the progress of humanity and is the foundation upon which all other spheres of society are built. On an individual level, education has the power to develop critical thinking, hone conflict resolution skills, and unveil each individual's essence. From a collective perspective, it can be used to nurture active, well-informed citizens concerned with the common good. Ultimately, it has the potential to generate economic development, reduce inequalities, foster ethical progress, and strengthen democracy, human rights, and the rule of law. The way children are educated shapes the potential for flourishing within any given population, so every decision made in this regard is highly consequential and political.

2. Especially since the COVID-19 pandemic, digital Information and Communication Technologies (ICTs) are increasingly present in the school environment. They are already used in children's admission tests at schools, in how teachers correct homework, in the personalization of learning content across various applications, as well as in school administration and security technologies. The use of learning platforms worldwide, mainly provided by companies from the United States of America (USA), China, and India, is also ever more common. Google Workspace for Education, Class Dojo, Carnegie Learning, IBM's Watson (in partnership with Pearson), Coursera, Blackboard, Udacity and Kahn Academy are just examples of the available diverse range of educational technology (edtech). Additionally, several others are gradually being adopted or are anticipated to be adopted in the near future, such as the use of large language models in adopted Artificial Intelligence (AI) systems, as well as the exploration of extended reality (XR) and the metaverse.

3. The opportunities brought about by edtech are tremendous, as they have the potential to transform education by expanding access to knowledge, improving the learning process, fostering conscious citizenship, enabling people with disabilities to access and enjoy the benefits of technology, and more. Goal 4 of the 2030 United Nations (UN) Agenda for Sustainable Development aims to "ensure inclusive and equitable quality education and promote lifelong learning opportunities for all" (Locatelli, 2018, p. 2). The Qingdao Declaration on ICT in Education of 2015 highlights how technologies can support the Sustainable Development Goals (SDGs) (Qingdao Declaration, 2015: Seize Digital Opportunities, Lead

Education Transformation, 2015). According to the declaration, technology is essential for strengthening education systems, ensuring universal access to education, promoting quality and effective learning, and facilitating equitable and more efficient service provision. More recently, the Beijing Consensus on Artificial Intelligence in Education (2019) recommended that governments and other stakeholders take action in various areas such as planning AI in education policies, AI for education management and delivery, and AI to empower teaching and teachers.

4. More specifically, the first obvious benefit of implementing digital ICTs in education is improving equality and inclusion. They can reduce the costs of accessing education for certain groups, such as those who live in remote areas, do not have access to schools, face learning difficulties, lack time, or have specific disabilities (Good, 2021; UNESCO, 2023b).

5. With the increased availability of information and knowledge online, students can access materials with even better quality than the ones they have access to in their region. Technologies can facilitate including students with special needs, support the diagnosis of disabilities, and adapt content to a way they can enjoy it. Examples include using AI to enable speech to text (and vice versa) or to generate automatic subtitles; supporting the socio-emotional and academic learning of autistic children; helping children with attention deficit hyperactivity disorder (ADHD); and, more importantly, “enabling students with special needs to study in a traditional (and inclusive) learning environment, which also changes peoples’ view on disability and special needs” (Vincent-Lancrin, 2021, p. 26).

6. Another promise of edtech relates to the use of early warning systems (EWS) for dropout prevention. An EWS is a tool developed to help identify students at risk of dropping out. Students are considered at risk when red flags, or specific indicators associated with dropout, are spotted. Examples include the cost of and structural issues within education, such as teacher quality and curriculum (United Nations Children's Fund (UNICEF), 2018). Technology-based EWS could effectively and promptly assist in addressing these specific needs.

7. Last but not least, edtech is also seen as a way to improve effectiveness and efficiency within education. Some argue that they can improve engagement as a prerequisite for meaningful learning and the development of cognitive and socio-emotional skills. Edtech could help identify engagement proxies (such as interaction patterns and eye, facial and body movements) as well as maintain it through nudging techniques (D’Mello, 2021). Educators’

jobs can get increasingly streamlined with automated systems built for reporting, resource allocation, and credentialing (Baker, 2021; Vincent-Lancrin, 2021). AI systems based on natural language processing can help correct exams or evaluate oral presentations; chatbots can help answer the most frequent students' questions; and predictive analytics promise to predict and assess students' progress throughout their academic life (Smuha, 2023b). Finally, edtech could improve public policies, driving transparent governance and better management of education systems and resources (Chakroun *et al.*, 2022).

8. The transformation of education promised by the benefits described above is, nonetheless, still far from being fully realized. Indeed, the adoption of edtech has brought about significant changes so far, introducing new ways to engage with educational content. The basic skills expected of current students also increasingly include those necessary to navigate the digital environment.

9. However, at this point, these changes can be considered incremental and uneven, with research showing that students can eventually experience more harm than good (Laird; Dwyer; Grant-Chapman, 2023). Their use and impact heavily depend on the socio-economic factors of the community where they are based, as well as the level of preparedness and willingness of the educators who implement them (UNESCO, 2023b, p. 6).

10. Differentiating the potential benefits, i.e., the ones claimed by their developers, and the evidenced benefits, which are supported by robust, independent scientific research on a significant scale is, therefore, key. Although thousands of studies have been carried out on the benefits of edtech, and more specifically on the use of Artificial Intelligence in Education (AIED), there is still little independent evidence of their effectiveness at scale, over time and across contexts (Holmes, 2023; Kucirkova; Brod; Gaab, 2023).

11. We should also consider the broader and often unforeseen side effects of edtech on children's human rights. This includes a significant increase in screen time, the widening of the digital divide between the privileged and underprivileged, the reinforcement of problematic pedagogical practices often focused on behaviorist mechanisms and techniques to capture children's attention, access to inappropriate content, and the rise of mis/disinformation. Historically marginalized communities also suffer disproportionate negative impacts (Laird; Dwyer; Grant-Chapman, 2023).

12. More specifically and important for this thesis, we must consider the effects that edtech has on children's rights to privacy and to the protection of personal data, whether as an end in

themselves or as a means to protect other fundamental rights such as non-discrimination, freedom of expression, personality development, autonomy, and human dignity. Children spend much of their time at school (in person or online) or working on educational activities. Therefore, the digital dossiers created about them while using these technologies have the potential to be highly detailed and comprehensive. This wealth of information can impact not only their performance at school and learning trajectories, but also their opportunities for university admission, entry into the job market, or even access to essential public services.

13. These technologies are also not introduced in a vacuum. The current educational system, whose main structures have changed little over the past centuries, is imbued with pedagogical and methodological discussions that interact with technologies in a unique way. As will be discussed throughout the thesis, important and influential trends in education, such as the measurement movement, align with the datafication processes of some technologies in a way that mutually reinforces each other. Similarly, discussions about the actors influencing educational decisions, which have always existed, intensify with the growth of neoliberalism and the increasing involvement of private actors in education through the provision of technologies.

14. This has intensified a narrative that the education sector is broken and stuck in the past (UNESCO, 2023b; Weller, 2014, p. 119); is lagging behind other sectors in adopting technologies (Allen, 2022; Pedro *et al.*, 2019); is under digitized; and “traditionally laggards when it comes to innovation” (Organization for Economic Cooperation and Development (OECD), 2021, p. 3). This discourse portrays the notion of development and enhancement of the educational framework as inherently reliant on technology. What is more, rather than addressing on the root of the problem, which is often the lack of sufficient financial and human resources, edtech has been seen as a magical way¹ to solve the educational crisis. This perspective has escalated a dangerous discourse of modernization at all costs and of technological solutionism (Morozov, 2014).

15. Discussing children’s experience with the digital environment and its impact on their education and broader development is key to understanding the future of individual and collective autonomy, as well as how citizenship is being transformed. If our intention is to maximize the benefits edtech has to offer, it should be assessed and deployed in a critical way,

¹ Sebastian Thrun, co-founder of online learning company Udacity Inc. and Stanford University research professor who helped create Google’s self-driving car, once said that “Education is broken. Face it. [...] It is so broken at so many ends, it requires a little bit of Silicon Valley magic” (Wolfson, 2013).

focusing on what is scientifically proven, on the educational goals we want to achieve, and on balancing the full array of positive and negative effects on children's human rights.

16. Based on the above, this research acknowledges the enormous potential that edtech can have in effectively transforming education, incorporating greater equity, quality, effectiveness and efficiency. Still, it views the current stage with rationality and scientific spirit, understanding what they can *actually* accomplish and balancing it with the risks they may still pose.

Research question and methodology

17. This section is dedicated to describing the research question that gave rise to this thesis, as well as the path taken to arrive at the outlined outcomes in its conclusion. Section a) will discuss the relevance of this research, why it was carried out, and how it contributes to the current state of the art. Section b) will focus on the research question that arises from the context described so far, as well as the sub-questions that resulted in the development of the respective sections of this thesis. Section c) will delve into the hypothesis formulated to help address the questions posed, serving as a compass to guide the research in a specific direction and methodology. Section d) will describe the scope of the research, and, finally, section e) will concentrate on the methodology used, as well as on the structure of the thesis.

a) Relevance

18. The incorporation of digital technologies in education is speedily expanding. With it, the edtech industry is also on the rise, already contributing around 6% of the global gross domestic product (GDP) (Pangarkar, 2023). The global education technology market is expected to be worth \$404 billion by the end of 2025 (HolonIQ Education Intelligence Unit, 2020) and \$700 billion by 2028 (Walker, 2023). This represents a significant surge compared to the projected valuation of \$76.4 billion for the worldwide education technology market in 2019 (Grand View Research, 2023). In 2021, the online learning platform Coursera, for instance, recorded 20 million new student registrations (Coursera, 2021), and there are at least 30 multi-million-dollar-funded corporations around the world focused on developing AI tools for education (Holmes, 2023, p. 64).

19. It is already a truism that technology is advancing too fast for the Law to keep up with it. The act of regulating presupposes evaluation and public discussion, which takes time and effort that are not proportional to the speed of technological change and innovation. Legal research is crucial to try to bridge this gap by analyzing the state of the art regarding the effectiveness of technologies in relation to what they aim to achieve and how they can affect the legal field. This includes understanding the objectives of education, particularly from a human rights perspective; examining the technologies' side effects, especially concerning children's privacy and data protection; striking a balance to maximize the benefits of technology while minimizing its harmful effects; and, finally, understanding the role of the Law in this equation and the available means to properly regulate technology.

20. To enhance digital readiness in education, the emphasis has been on expanding connectivity, digital infrastructure, and online tools. Nevertheless, aspects such as privacy, data protection, governance, and security have been somewhat neglected (Chakroun *et al.*, 2022). Considering that the global adoption of digital ICT and AI in education is a relatively recent phenomenon, which has intensified with the COVID-19 pandemic, it is necessary to understand whether the current legal framework is sufficient to address the presented challenges. More specifically, we should explore how we can maximize the effects of the available legal tools, such as the Convention on the Rights of the Child (CRC), data protection and procurement frameworks, to handle these challenges without waiting for new laws to be implemented. At the same time, we should map what is out of their scope and assess whether and how the Law should further regulate these issues, if at all.

21. This is only possible by understanding the Law as an applied social science, whose effects on individuals and groups must be grasped empirically and contextually. The cold text of the law tells us little about its real effects on society, and thus a comparative and bottom-up approach to the problem can be beneficial. Despite the existence of research on the risks stemming from specific applications of edtech, there still remains a gap in comprehensive analysis. This thesis therefore contributes to the existing body of knowledge by broadly mapping the risks that edtech can pose to children's rights to privacy and to the protection of personal data in Brazil and the European Union (EU), based on a transdisciplinary literature review and empirical analysis of a case study.

b) Research question(s)

22. The main question that guides this research is: *What are the challenges that edtech presents to children's rights to privacy and to the protection of personal data, and to what extent does the current legal framework in Brazil and Europe address them?*

23. This question can be broken down into several sub-questions, which will ultimately steer the development of the research and the unfolding chapters of the thesis:

- i. What can be understood by edtech, and what are its main purposes?
- ii. How does edtech, with its logic and design, interact with the concept of education and the long-standing discussions and theories carried out in this sector?
- iii. Based on its main uses and technologies encompassed by the concept of edtech, how does it affect children's rights to privacy and to the protection of personal data?
- iv. How do the EU and Brazilian legal frameworks currently regulate children's rights to privacy and to the protection of personal data?
- v. Drawing on insights provided by the theory of data colonialism, is the current legal framework sufficient to address all the mapped challenges?

c) Hypothesis

24. Due to its comprehensive nature, the concept of edtech encompasses vastly different technologies both in terms of purpose and technical aspects. This results in diverse conditions under which they are used and different risks that could undermine children's rights. However, through the development of a typology, it is possible to identify commonalities among them that would warrant their collective consideration.

25. Considering the existing literature and the theory of data colonialism, the first part of the hypothesis of this research posits that the prevailing business model of digital platforms, characterized by the escalating datafication of human life and social interactions, particularly in the feeding of AI systems, as well as the commodification of data, engender several challenges surrounding the use of edtech concerning children's rights to privacy and the protection of personal data, including the intensification of surveillance, the reinforcement of

historical inequalities, the severe impact on life opportunities, the manipulation of individuals and groups, and ultimately, the erosion of digital sovereignty.

26. Although many of these challenges can already be addressed by the current legal framework, such as through data protection regulation, the latter's primarily procedural focus does not thoroughly considering the purposes for which data can be processed in the first place, and are not completely equipped to deal with the specific challenges posed by AI. Therefore, the second part of the hypothesis to be tested is that the EU and the Brazilian frameworks, including the application of oversight mechanisms, do not address some of these challenges. Because of historical inequalities between the two jurisdictions and the added layers of vulnerability inherent in Brazilian reality, the enforcement of existing rules is further hindered in the latter.

d) Scope of the research

27. **Technical Scope:** The analysis carried out throughout the thesis will be focused on data-driven edtech, encompassing technologies that collect, analyze, and make decisions based on (personal) data that affect people's lives. These activities can be executed through traditional data analysis technologies, using statistical methods and other mathematical techniques to recognize patterns, discover relationships and gain other insights from data. Nonetheless, this has increasingly been done by AI, including symbolic AI techniques or, more commonly (and also more heavily dependent on data), Machine Learning (ML) techniques. The latter will therefore be the main source of challenges to be discussed in Part III of the thesis. Within data-driven edtech, I will present a typology that differentiates between edtech used for *providing education* and for *learning about education* in Chapter 1.

28. **Legal Scope:** The focus of this thesis, concerning legal analysis, is on children's rights to privacy and to the protection of personal data. However, I acknowledge that human rights are indivisible and interdependent. In order to protect these two rights, others must be realized. Similarly, safeguarding the privacy and data of children is essential for the fulfilment of other rights. I therefore adopt a children's rights perspective regarding privacy and data protection rights, aiming to understand this complex framework in a holistic fashion.

29. **Geographical scope:** Technologies are social-technical artifacts that directly interact with the specificities of the communities in which they are embedded. Recognizing the need to analyze this socio-economic context beyond the legal framework, and understanding that the

operations of edtech companies are generally global, this research will focus on two different jurisdictions: the EU and Brazil. As will be later discussed, data protection laws in these two jurisdictions are remarkably similar as a result of the Brussels effect. However, changes in context result in distinct enforcement of these rights and varying effects of technologies within communities. Therefore, rather than a mere legal comparison, which could obscure the concrete application and effects of the Law in society, the aim is to compare socio-economic contexts and how they influence the application of data protection laws. This will be carried out within the context of a case study of Google Workspace for Education, as more thoroughly detailed in Part III of this thesis. The choice to analyze Brazil and the EU stemmed from the geographical location and past experiences of the doctoral candidate. Considering the context of the Joint PhD between the State University of Rio de Janeiro (UERJ) and KU Leuven in which the research was carried out and the fact that these two jurisdiction are part of different spectrums of social reality, the analysis of both situations had the potential to bring a wealth of important insights to the case study. Google Workspace for Education operates globally, yet its social impacts vary significantly across different parts of the world.

e) Methodological approach and thesis structure

30. In order to address the research question and sub-questions presented in Section b) and test the hypothesis outlined in Section c), this thesis employs various complementary and interrelated methods.

31. After this introduction, **Part I** will be developed through a *descriptive approach*, setting the stage for the subsequent analysis. Three chapters will be presented to elucidate the current context in which edtech is developed and deployed.

32. **Chapter 1** will focus on introducing what edtech means. It will offer a historical overview of its evolution to date, aiming to describe not only the journey leading to the technologies currently employed but also how methodologies and theories developed for conceptualizing preceding technologies help us comprehend the functioning and constraints of the current ones. I will additionally present a typology to synthesize and organize the complex landscape surrounding edtech. Although developed only for didactical purposes, this typology will be crucial for understanding the purposes for which these technologies are used and who they support, which directly changes the risks they present to children's rights.

33. **Chapter 2** aims to explore the interaction between the implementation of edtech and longstanding discussions within the field of education. This encompasses the role of the private sector in providing products and services, and, consequently, influencing strategic decisions in education; the phenomenon of “learnification” of education and discussions regarding what is to be “efficient”; the measurement movement in education and its relationship with datafication; as well as the dynamics of platform learning. The importance of this chapter for legal analysis extends beyond identifying the network of actors involved in providing education and their respective interests. It also involves understanding how the integration of edtech into these discussions can amplify specific challenges related to children’s privacy and data protection.

34. **Chapter 3** will introduce data colonialism as the theoretical and normative framework adopted by this research, as described by Couldry and Mejias (2019). This chapter will outline the primary components and actors within data colonialism, illustrating its disproportionate impact on certain individuals and communities, particularly children, and examining its effects on both individual and collective autonomy. Together with the legal framework, this theory will serve as a normative lens to evaluate the deployment of edtech and the challenges it poses to children’s rights in Part III. It can also thus help assess the sufficiency of the current legal framework to deal with these challenges.

35. **Part II** is focused on *describing and evaluating* how the current legal framework regulates children’s rights to privacy and to the protection of personal data.

36. **Chapter 4** will present the literature on the reasons why children require special consideration when it comes to protecting their rights to privacy and to the protection of personal data. Their status as human beings in development and their proportionally larger digital footprint compared to adults will be highlighted as crucial fundamentals for this special treatment. This chapter acknowledges the importance of viewing technologies not only through a lens of risk and protection but also as a means for opportunities and developing children’s autonomy. Considering the scope of the thesis, which is focused on identifying the main risks that edtech poses to children’s rights to privacy and data protection, the chapter will introduce a risk classification of children’s online presence, highlighting how surveillance technologies can significantly impact children’s development and learning. However, it also highlights how edtech has a critical role in realizing different human rights, when deployed in a way that respects children’s specificities.

37. **Chapter 5** will present the CRC as a fundamental human rights framework adopted by Brazil and the EU, which recognizes children as rights holders and holistically address the specificities mentioned above. This chapter will present the main provisions in the Convention applicable to the scope of this thesis and how some cross-cutting standards (should) influence the interpretation and implementation of the legislative and policy pieces discussed in the following chapters. **Chapters 6 and 7** will respectively describe and evaluate the EU and Brazilian legal frameworks dealing with children's rights to privacy and data protection, as well as applicable policy to edtech.

38. It should be highlighted that this thesis will not adopt a traditional legal comparative methodology, as mentioned above. Comparisons between the EU General Data Protection Regulation (GDPR) and the Brazilian General Data Protection Law (*Lei Geral de Proteção de Dados Pessoais* - LGPD), in particular, are inevitable due to the considerable similarity between these legal frameworks. However, the thesis' aim is to focus on the social contexts of the application of each law. I will outline some challenges brought by a mere legal transposition of European legislation without necessarily considering Brazilian specificities, especially regarding its institutional design. This will be done in a contextualized manner in Part III of the thesis through a case study, which attempts to discuss how these aspects influence the protection received by data subjects, even with such similar laws being implemented.

39. **Part III** will be formulated based on a *descriptive, evaluative and normative* approach and it has two main focuses. First, **Chapter 8** will map challenging aspects that data-driven edtech raises to children's rights to privacy and to the protection of personal data. I will outline the risks posed by AI systems in general and their intersection with education. Afterwards, I will highlight certain technologies as presented in the developed typology and discuss how particular challenges can be identified in their implementation.

40. The second focus is a case study of the application of Google Workspace for Education in the EU and in Brazil. Google pioneered the development of data-driven business models (DDBM) on the scale that we currently know and Google Workspace for Education is largely adopted worldwide. This model has been widely replicated by other edtech, and even when schools adopt technologies from different companies, Google is still often involved in a broader network of data sharing. Studying Google's dynamics can thus provide a framework to understand other commercial edtech and their impacts on children's rights. Furthermore, in recent years, particularly amid the COVID-19 pandemic, European Data Protection Authorities

(DPAs) have been actively involved in cases related to this technology. This engagement offers valuable insights into its operation and the challenges stemming from its implementation.

41. **Chapter 9** will describe how Google Workspace for Education works, the history of its development, and how it is related with the overarching Google's business model.

42. **Chapter 10** examines its impact on children's privacy and data protection in the EU and in Brazil. First, I describe decisions made by authorities of different EU Member States (MS) that involve the use of Google Workspace for Education by public schools. Considering the auditing and analysis capabilities of certain authorities, especially DPAs, it is possible to have a more in-depth view of the risks, which the mere assessment of Terms of Service (ToS) and Privacy Policies would not provide.

43. The chapter also discusses the implementation of Google Workspace for Education in Brazil. Since the Brazilian DPA has not yet assessed it based on the Brazilian framework, an analysis of the ToS and Privacy Policies applicable to the platform in the country will be conducted. This will be complemented by a literature review on research that have also performed a similar exercise.

44. **Chapter 11** undertakes an analysis of the collected information from both jurisdictions, aiming to understand the systematic functioning of Google Workspace for Education beyond compliance with the GDPR and LGPD, within the context of data colonialism and the application of AI technologies. Initially I will evaluate the similarities, differences, and deficiencies apparent in the current landscape, drawing upon the insights provided in Chapter 10. I will then discuss how data colonialism's main aspects can be identified in the case study. This chapter also assesses the extend to which legal frameworks for personal data protection in the EU and in Brazil deal with such challenges.

45. The thesis will be wrapped up with **concluding remarks, recommendations, and indications for future research**. In addition to summarizing the results of the thesis, this section will present its conclusions, high-level recommendations on how to move forward in relation to the identified challenges, as well as topics for future research.

46. Finally, it is important to mention that this thesis follows the author-date citation style of the Brazilian National Standards Organization (*Associação Brasileira de Normas Técnicas* - ABNT), as adopted by UERJ, the host university.

PART I. SETTING THE SCENE

47. Part I adopts a descriptive approach aimed at laying the context for the legal analysis. To map out the effects that edtech has on children's rights to privacy and to the protection of personal data, it is first necessary to understand what type of technologies are under the scope, what educational context they are inserted into, and which theory will be used to interpret these effects.

48. Chapter 1 will thus provide the history of the development of edtech, as well as a possible definition of it. Reflecting on the past is beneficial not only for understanding our current position and the reasons behind certain phenomena but also for learning from mistakes to prevent their recurrence. Building on this historical background and the literature review, this chapter also introduces a typology of edtech based on their purpose and target audience. This typology will serve as a framework in the final part of this thesis to analyze the risks associated with specific technologies.

49. Chapter 2 acknowledges that edtech is not deployed in a vacuum and that education, in general, and pedagogy, as a specific science, are imbued with centuries-old discussions about how education and learning should be carried out. Technologies are never neutral and will reflect the worldview of their developers, as well as their vision of how education should take place. The risks presented by edtech are therefore also influenced by their interaction with the context in which they are deployed, as well as their leading actors.

50. Finally, Chapter 3 discusses data colonialism as the theoretical and normative framework adopted by this thesis. This theory provides us with important insights to understand risks that may still be present even if the current data protection laws are complied with.

Chapter 1. The use of technology in education

51. The history of edtech is intertwined with the history of humanity's relationship with knowledge. What this timeline includes, therefore, greatly depends on the very definition of education, of technology and, consequently, of edtech.

52. Education is often understood as the discipline “concerned with methods of teaching and learning” or with “the transmission of the values and accumulated knowledge of a society” (Lawson *et al.*, 2023). It can also be seen a process involving “activities aimed at the development of productive, thoughtful, and responsible persons. These activities result in learning, or stable and persisting changes in what a person knows and can do” (Spector, 2015, n.p.). These two definitions share the idea that students are educated either to acquire knowledge or to develop a particular skill. Even in the second definition, where educational activities include the development of productive, thoughtful, and responsible people, the emphasis is still on what a person can know or do and not necessarily on what they become.

53. With a broader and more critical view, Paulo Freire, a Brazilian pedagogue, understands education as a process of knowledge development, political formation, ethical manifestation, pursuit of beauty, scientific and technical empowerment (Freire, 2001). Freire understood History as a possibility, as something in motion that can actually be changed. This does not deny the role of the conditioning factors to which humanity is subjected. However, by opposing the future as something inexorable, the notion of History as a possibility recognizes the importance of human decisions as acts that imply rupture. It acknowledges the importance of consciousness and subjectivity, of the critical intervention of human beings in the reconstruction of the world (Freire, 2001). Education, therefore, plays a decisive role in the transformative path towards critical individuals and more politicized, democratic, equalitarian and empathetic societies.

54. This broader understanding of the aims of education is aligned with the ones defined in arts. 28 and 29, CRC, as will be discussed in Part II, of this thesis. Focusing on the transformative and multiplier role of education is essential to gauge the power that edtech has in shaping it. If we fail to promote a suitable environment to achieve these goals, we risk hindering the development of both individuals and society as a whole. This already demonstrates the need to treat education as a strategic and inherently public good which demands transparent, democratic and fair decisions.

55. Akin to education, the concept of technology has also been contested throughout history. Saettler (2004, p. 3) understands technology² as “a system of practical knowledge not necessarily reflected in things or hardware” (Saettler, 2004, p. 3). In the same vein, for Spector (2015, n.p.), technology would be “the systematic and replicable application of knowledge to achieve a purpose. Some technologies can be seen and touched (e.g., computers), whereas others are in the form of specific ideas and methods (e.g., a sorting algorithm)”.

56. On the other hand, Salomon (1984) argues that the use of the word technology to define technical arts themselves more than the *discourse* on the technical arts is recent. According to the author, this happened mainly when these artifacts started to become something other than arts but a scientific endeavor.

57. The author stresses the importance of differentiating *technology* from *technique*. The English language has no real equivalent of the word technique as used in French, German and Slavic languages. In these languages, more than something related to skills or methods, technique refers to all activities associated with things technical. Therefore, he argues that the changes introduced mainly from the XIX century onwards, when science and technical arts became more connected, are fundamental to the very meaning of technology (Salomon, 1984).

58. It is not under the scope of this thesis to dig deeper into this discussion. Indeed, what is commonly called edtech today will more often than not be related to this more refined state of *technique*, as “the application of *scientific knowledge* to the practical aims of human life” (The Editors of Encyclopaedia Britannica, 2022, emphasis added). This is what will then inform the concept of edtech as described below. However, for the purposes of understanding the history of edtech, some educational *techniques* would also be considered to set the scene for the following developments.

59. As becomes clearer with the different views on education and on technology, there is also no single and uncontroversial way of defining edtech, and many of the existing definitions contradict each other (Czerniewicz, 2010). Based on the definition of education by Freire and the broader understanding of technology, edtech will be understood in this thesis as the application of scientific knowledge to support both the acquisition of knowledge and skills, as well as the development of critical, ethical, and socially responsible individuals.

² From the Greek form *techne*, translated as art, craft, or skill plus *logos*, Greek for word, study or knowledge.

1.1 A brief history of edtech

60. In this section, I will present a brief overview of the historical evolvement of edtech. Looking at the past is an important exercise to gain insights into the trajectory of current edtech, appreciating the challenges, advancements, trends and patterns that influence how we understand the role of edtech in our current society and how they can better serve children and education. However, it is not my intention to tell the story of edtech as something that builds up to the introduction of computers or AI, which are often seen as the pinnacle of this progression.

61. Watters (2019) warns that this kind of thinking runs the risk of suggesting that education has become increasingly and *necessarily* technological over time. It can portray the digital classroom as an inevitable outcome, promoting a vision of teaching and learning that heavily rely on technology (Watters, 2019, parag. 1). The use of technology in education is truly promising and has the potential of realizing several fundamental rights, as emphasized in the introduction. However, as this thesis will argue, there is still a tendency to advocate for the use of technology for its own sake without engaging in a broader discussion about its alignment with predefined pedagogical goals and its necessity and proportionality when its benefits are weighed against its side effects.

62. To view these historical developments in such a teleological manner would prioritize the role of technology at the expense of other social, economic, or political issues that played a significant role. Each technology has its own value and was/is important for its own reason. Unfortunately, it is not feasible to cover all the political, social, and economic aspects of each development. Nonetheless, this disclaimer is necessary for the critique that will follow later in the thesis and for encouraging readers to explore these developments and their implications further through the literature cited in this work.

63. It is also worth noting that while edtech is ubiquitously present in all continents, its development and application have not been uniform. The COVID-19 pandemic has exposed significant disparities in the access to technologies used to maintain learning processes, which are often dictated by technical and financial constraints (UNESCO, 2023a).

64. This overview, therefore, will primarily focus on the moment of the emergence of the respective technologies. This approach is not without its problems, considering that, for the most part, the technologies mentioned below were primarily developed and used in Europe and

the USA before spreading to the rest of the world. Thus, the use of some of these technologies in other regions, especially in Brazil, as well as some of the consequences of importing this technology, will be discussed later in this thesis. The history below is also not intended to be exhaustive; rather, its purpose is merely illustrative, highlighting key milestones that influenced the way current edtech is developed and deployed, as well as societal perceptions surrounding them.

65. The use of practical ways to transmit knowledge and to improve learning can be traced back when tribal priests systematized knowledge or when pictographs were used in early cultures. The very development of writing—such as the Sumerian script and the Egyptian hieroglyphics—can be considered as one important way to facilitate communication and education. Other instruments, such as the abacus³, analogue computers⁴ and the quill pen⁵, were also gradually introduced.

66. The invention of the printing press was undoubtedly a watershed in history. It made it possible for previously laboriously handwritten books to be produced quickly and at scale, which increased access to knowledge like never before (Saettler, 2004). With the spread of written knowledge, there was also an expansion of formal education in Europe, which led to the Renaissance and the Enlightenment periods.

67. In 19th-century Europe, improvements in transport infrastructure led to the development of the first distance degree program in the University of London in 1858 (Bates, 2019). In 1873, a network of women teaching other women through the mail was founded by Anna Eliot Ticknor, the Society to Encourage Studies at Home (Briggs, 2014). During this period, technologies such as lantern slides also began to be utilized in the USA, particularly for adult education, thus initiating the visual education movement (Saettler, 2004).

68. At the end of the 19th century and the beginning of the 20th century, the invention of the motion picture profoundly accelerated the use of technologies in education and its effects are still felt today. The great potential that this new technology could have for education was already perceived in the 1910s, both in Europe and in the USA. In 1911, Thomas Edison was

³ The abacus is a calculating tool used at least since 480 BC by several cultures such as the Egyptians, the Greeks and Chinese (Briggs, 2014).

⁴ Several mechanical analogue computers were developed in ancient times for astronomical calculations such as the astrolabe and the Antikythera mechanism (Briggs, 2014).

⁵ The quill pen was usually made from a bird feather and were introduced around 700 AD (Briggs, 2014).

one of the pioneers in producing films for the educational setting, having released a series telling the story of the American Revolution (Saettler, 2004).

69. In the New York Dramatic Mirror's issue of July 9, 1913, Edison prophesied that books would become obsolete in schools: "[s]cholars will soon be instructed through the eye. It is possible to teach every branch of human knowledge with the motion picture. Our school system will be completely changed in ten years" (Edison, 1913, n.p., as cited in Saettler, 2004, p. 98). This drastic change was not possible in 10, but certainly in 100 years. A century later, as will be described below, Massive Open Online Courses (MOOCs) would become extremely popular.

70. At Columbia University, Professor Ben D. Wood, together with University of Chicago Professor Frank Freeman, conducted a study with around 11,000 students involving the use of films in geography and general science classes. The results showed that students who were taught using films scored higher on end-of-unit assessments than those who were taught using printed materials. The study's findings suggested that using teaching films could be a successful way to enhance the effectiveness of traditional pedagogical methods in schools (Watters, 2021, p. 64–65).

71. According to Wood, schools should be more attuned to the individual needs of students. In order to achieve this goal, however, the education system should transition to what he referred to as "mechanical education", which is not to be confused with a mechanistic approach.

Perhaps this seems counterintuitive: to individualize education, one must automate it. To resist mechanistic education, schools must mechanize. But for education reformers in the early twentieth century (as for those in the early twenty-first), it was a conundrum they managed to justify. Indeed, this contradiction gets at the heart of calls for "personalization" and is central to a vision—then and now—of a modern, high-tech, progressive learning experience (Watters, 2021, p. 68).

72. The 1920s saw the emergence of educational radio (Saettler, 2004). Although its popularity dropped, especially with the rise of television broadcasting in the mid-XX century, it is still important for educational purposes in various parts of the world (see, for example, Damani and Mitchell (2020)). This was an important milestone for the history of edtech, since it marked the introduction of ICT in education (UNESCO, 2023b).

73. It was also in the 1920s that the first paper on and a prototype of an "automatic teacher" was presented by Ohio State University's Professor Sidney Pressey in the joint meeting of the American Psychological Association (APA) and the American Association for the Advancement of Science of 1924 (Watters, 2021, p. 35–36). The machine had various versions, but the most sophisticated one was based on a typewriter. While working on a set of questions

on a printed sheet, the student would use the device's keys to choose their answers. The system was designed to immediately inform students whether their selection was correct, and it impeded them from proceeding to the next question until they had it right (Holmes; Bialik; Fadel, 2019). As will be discussed in the last part of this thesis, this strategy is still highly used by current personalized learning technologies.

74. His initial attempts to put the device on the market and later to keep it were not successful for many reasons, but he continued his academic research on the topic. He was one of the first to argue that “[u]nlike the ‘mass education’ of the radio or the film projector, [...] his Automatic Teacher would foster a more individualized classroom [...] and free the teacher from the mechanical tasks” (Watters, 2021, p. 44–45).

75. The first typewriter was developed in 1868 (Cortada, 1993), and in the early 1890s, William A Mowry and Frank Palmer already advocated the use of the machine in secondary schools. However, it was not until 1932 that Professor Ben D. Wood, once again working alongside Professor Frank Freeman, conducted research that demonstrated the benefits of using typewriters in classrooms, including enhanced reading habits among students and an increase in the amount of written work produced. This ground-breaking study paved the way for widespread acceptance of typewriters in the classroom, and subsequent research further confirmed their advantages for learning (Cothran; Mason, 1978).

76. As a consultant to the International Business Machines Corporation (IBM), Professor Wood was also responsible for using machines to analyze test scores. In 1932, an IBM tabulator was adapted to score the Strong Vocational Interest Blank, a test used for student counselling that was previously costly to grade and analyze. A few years earlier, Reynold B. Johnson, had developed his own test scoring machine, the so-called “Markograph” and was afterwards hired by IBM. IBM developed the first commercial test-scoring machine in 1938 (Watters, 2021, p. 72–73).

77. Although IBM's scoring machines were not a commercial success, they influenced the testing industry and the way education was viewed.

Just as Wood's work with the typewriter industry had likely decreased those companies' interest in manufacturing the machine that Pressey had designed, Wood's work with IBM seemed to convince the company that “mechanical education”—individualized education—was to be achieved through large-scale data analysis and testing machines (Watters, 2021, p. 79).

78. In the 1940s, the invention of the television was seen as a solution to several issues within the educational system, such as teacher shortages and overcrowded classrooms. In the

USA, the introduction of classroom-based instructional television in 1947 by the Philadelphia school district marked a ground-breaking initiative and involved broadcasting one educational program per week. During the 1950s, the first educational television programs designed for public broadcasting were developed (Levin; Hines, 2003, p. 264).

79. The City Colleges of Chicago took a pioneering step in 1951 by establishing a comprehensive system for large-scale instructional television programs that offered academic credit. This innovative approach allowed students to earn a degree solely by enrolling in television courses (The Education Coalition, [s. d.], n.p.). In Europe, television was first used in the 1960s for educational purposes (Bates, 2019).

80. In 1953, after visiting his daughter's fourth-grade math class, Harvard psychology professor B. F. Skinner was surprised by the way children were being taught. The students were seated at their desks, solving arithmetic problems displayed on the blackboard. The teacher moved between the rows of desks, observing the students' work and correcting their mistakes. Some students finished quickly and awaited the next set of instructions, while others struggled and were frustrated. After the lesson, the teacher collected the papers to grade and returned them to the class the next day (Watters, 2021, p. 19).

81. This violated the basic principles of Skinner's behaviorist theory of learning and tried to adapt the experiments he has been carrying out with rats and pigeons to people. He tried then to build teaching machines, continuing the work of Sydney Pressy in the 1920s. In one of the models, paper disks containing questions would show up in one window, while the student would write their response on a roll of paper through a second one. The mechanism would automatically hide the student's answer, preventing any alterations and simultaneously unveiling the correct one. This way, Skinner's teaching machine delivered automatic and immediate reinforcement to students (Holmes, 2023, p. 95–96).

82. In regular classrooms with human teachers, they would move too fast for some students and too slow for others. Therefore, Skinner thought that machine instruction would be the solution for students to move at their own pace. This would realize the “industrial revolution in education” and make it more efficient (Skinner, 1958, p. 969). Although some would see this as a way of implementing mass production, Skinner was of the opinion that the machines could rather act as private tutors. His view deserves to be cited in full length:

(i) There is a constant interchange between program and student. Unlike lectures, textbooks, and the usual audio-visual aids, the machine induces sustained activity. The student is always alert and busy. (ii) Like a good tutor, the machine insists that a given point be thoroughly understood, either frame by frame or set by set, before the

student move on. [...] (iii) Like a good tutor, the machine presents just that material for which the student is ready. [...] (iv) Like a skillful tutor the machine helps the student to come up with the right answer. It does this in part through the orderly construction of the program and in part with techniques of hinting, prompting, suggesting, and so on, derived from an analysis of verbal behavior. (v) Lastly, of course, the machine, like the private tutor, reinforces the student for every correct response, using this immediate feedback not only to shape his behavior most efficiently but to maintain it in strength in a manner which the layman would describe as “holding the student’s interest” (Skinner, 1958, p. 971).

83. The resemblance with today’s intelligent tutoring systems (ITS) and with the rationale behind edtech is surprising, although not a coincidence. Like teaching machines, current edtech, especially the ones built for personalized learning, intends to present the content according to each student’s level. They use nudges and other psychological mechanisms to guide learning and seek to reinforce certain behaviors to hold students’ attention. This shows how much the current technology is still based on behaviorist approaches of learning instead of more progressive ones.

84. Skinner’s work has laid the foundation for the functioning of current edtech, especially the ones powered by AI. However, the teaching machines cannot be said to be adaptive, as students would go through the same set of questions and content, although at their own pace. This feature was what Gordon Pask tried to implement also in the early 1950s. SAKI, the self-adjusting keyboard tutor, was created to assist keyboard operators in mastering the use of a card-punching device for data processing. The assigned exercises were tailored according to the learner’s unique progress, as indicated by a dynamic probabilistic student model (Holmes; Bialik; Fadel, 2019, p. 98).

85. The rapid development of ICTs in the second half of the 20th century dramatically changed how humanity deals with data and knowledge, bringing new perspectives to the educational sector. The rise of personal computers (PC) in the 1970s and 1980s made this technology more accessible, especially in Europe and the USA. In 1971, Michel S. Hart typed the text of the United States Declaration of Independence and transmitted it to others in the computer network he had access to at the University of Illinois. It was the first document of what would become the Project Gutenberg⁶.

86. After the Apple II’s release in 1977, the Minnesota Education Computing Consortium procured 500 computers to distribute among schools in the state. In the 1980s, Apple initiated a campaign to promote the usage of their computers in American public schools. They actively

⁶ Project Gutenberg is the first online library of free eBooks to be ever established (Project Gutenberg, [s. d.]).

lobbied for the passage of a bill in the US Congress and in California to support their cause. In California, a bill was passed granting a 25% tax credit against the state corporate income tax for computer equipment donations to schools. Taking advantage of this incentive, Apple donated a computer to each of the approximately 9000 eligible elementary and secondary schools in California. This significant expansion into California's educational institutions, combined with the launch of the Macintosh in 1984, led to Apple's rapid domination of the education PC market, at least for a certain period (Watters, 2015).

87. In Finland, the subject of “automated data processing” was introduced in schools. Programming was not being taught to train programmers, but rather to develop student's logic and math skills (Leinonen, [s. d.]). However, with all the challenges that computers raised at that moment, teachers who constantly used them in their classrooms were the exception (Corcoran, 2013).

88. At this stage, pedagogical thinking was often based on Computer-based Training (CBT)⁷ or Computer-based Learning (CBL)⁸, types of Computer-Aided Instruction (CAI), where the interaction would occur between the student and computer drills, micro-worlds and simulations. However, these programs lacked adaptability, which Jaime Carbonell attempted to implement through a system called SCHOLAR in 1970. This is known to be the first implementation of AI in CAI (Holmes; Bialik; Fadel, 2019, p. 100).

89. A second phase of the history of computers in education began in the late 1980s and early 1990s when multimedia computers came to the mass market. Multimedia was seen as a method to cater to the different ways people learn (Leinonen, [s. d.]). The advent of the Compact Disc-Read Only Memory (CD-ROM) was probably the first way most people came into contact with educational programs for computers.

90. The popularization of the World Wide Web in the mid-1990s, even with the simple design characteristic of Web 1.0, created many opportunities for education. First, it removed

⁷ CBT is an interactive instructional approach in which the computer, taking the place of an instructor, provides a series of stimuli to the student ranging from questions to be answered to choices or decisions to be made. The CBT then provides feedback based on the student's response (Computer-based training, 2009).

⁸ “Computer-Based Learning has emerged in response to Computer-based training (CBT) and as its name it is more focused on Learning. [...] The 1980's and 1990's produced a variety of schools that can be put under the umbrella of the label “Computer Based Learning” (CBL). Frequently based on constructivist and cognitivist learning theories, these environments focused on teaching both abstract and domain-specific problem solving. Preferred technologies were micro-worlds (computer environments where [sic] learners could explore and build), simulations (computer environments where learner [sic] can play with parameters of dynamic systems) and hypertext” (Computer-based learning, 2009, n.p.).

the filter of knowledge publication and for this alone it can be considered the most significant socio-technological change since the invention of the printing press. With the wikis at the end of the 1990s, this process became collaborative, a shared enterprise. Second, it made communication (such as between researchers) easier. Teaching resources also began to be shared, which started the open education movement (Weller, 2020).

91. As with almost anything in this period, learning gained its *e-* form. The concept of e-learning started to spread, and although it initially covered any use of electronic media in learning, its interpretation gradually narrowed down to online learning (Weller, 2020). The hype around e-learning, however, also presented its challenges. With e-learning, the e-learning industry and markets for courses and systems emerged. However, many of these offerings were developed without a thorough prior assessment of their actual need and purpose (Leinonen, [s. d.]). As often happens with other edtech, they

were shown to be designed primarily to prove their success rather than to find solutions to perennial educational problems. The prevailing impulse of these innovations and reforms [was] characterized solely by a desire for improvisation and typically they lacked any sound theoretical or experimental foundation (Saettler, 2004, p. 399).

92. Around 2002, Learning Management Systems (LMS), or Virtual Learning Environments (VLE), became the dominant and most successful edtech. They were created to be the central e-learning technology, and it dismissed the need to use several tools at once, such as bulletin boards for communication, content management systems and web pages (Weller, 2020). In the beginning, LMS were often used as a virtual replica of the physical classroom, where lectures and notes would be uploaded without much experimentation in terms of pedagogy. Its true potential was only realized with time.

93. In terms of terminology, the term VLE has been criticized because of the word “virtual” and of the idea that “learning through such an environment is a poor relation to any learning that takes place in a face-to-face setting” (Weller, 2007). With the intense increase in the number of sensors implemented in physical spaces, the existence of a virtual world was also contested, since it could imply that it is not real or its consequences not as tangible. On the other hand, LMS has also been objected due to the suggestion that it could manage students’ learning, which would not be aligned with more exploratory and constructivist pedagogies (Weller, 2007). Ultimately, however, these two terms have been used interchangeably and can be considered synonyms.

94. Around 2007, there was a peak of interest in the so-called online virtual worlds, especially by higher education institutions. The platform Second Life was particularly popular and universities would lease islands to create their own virtual environment through avatars. At the time, it was mainly used for lectures, and it could be integrated with other technologies such as the LMS Moodle (Weller, 2020).

95. Weller (2020) notes that, although the expectations were very high, they did not gain much traction. First, there was a lack of imagination on how to use it beyond lectures. If that was the main goal, regular streaming technology could be used instead. Second, it required good computer hardware and internet broadband, which was not the case for all students and schools. There was also the problem related to abusive behavior, such as virtual vandalism or classroom interferences. In terms of accessibility, some students were not able to use the online environment due to visual impairments. This is as a prime example of technology being used for its own sake, taking precedence over serving a pedagogical purpose (Weller, 2020). These ideas are currently reflected in the use of the metaverse in education, as will be further discussed below.

96. The rise of online worlds has also emphasized the use of games for educational purposes, as well as the implementation of gamification design patterns in edtech more broadly. Gamification can be understood as a “design strategy used to promote engagement and activity across a wide range of digital products and services” (5Rights Foundation, 2021, p. 34) and is increasingly used in education. Digital badges, for example, became a trend in 2015 and are used to digitally represent skills or experiences acquired by the student (Weller, 2020). With different technologies competing for children’s attention and with the increasing implementation of stimuli for completing tasks (highly linked to behaviorist views of education), gamification strategies are increasingly present in edtech.

97. By 2011, with the plethora of services available for learning, a new movement began gaining traction. The collection of the various support tools used by learners and educators came to be known as “Personal Learning Environment (PLE)” and it was seen as a way to enable learners’ control and personalization. Instead of a single LMS technology universally used by all, PLEs could be built by learners themselves based on their needs. Initially conceptualized as simple diagrams illustrating the tools individuals employed within their learning contexts, discussions quickly shifted toward the potential integration of data from these diverse platforms (Weller, 2020).

98. Despite various factors leading to the eventual waning of the PLE hype, personalization has remained a coveted goal in education. The SCHOLAR system, as previously described, is considered to be the first ITS, which is the base for the majority of the technologies used for personalized learning today.

99. 2012 was declared by The New York Times as the year of MOOCs (Pappano, 2012). Although the idea of running open courses was not something novel by this time, the convergence of some technologies as well as the sudden popularity of Stanford professor Sebastian Thrun's course on AI attracted all possible headlines (Weller, 2020). Many have portrayed MOOCs as revolutionary technology, but they did not live up to all expectations. Among the emerged issues were low competition rates, lack of demographic diversity (most participants were already educated) and lack of a sustainable business model. Over time, MOOC providers began integrating e-learning within traditional education systems and underwent changes to their business models.

100. From a strictly educational point of view, MOOCs offered numerous advantages, including the expansion of learning opportunities and open practices (even if this is the case only for enrolling and not for licensing) (Weller, 2020). However, the rise of MOOCs revealed a deeper attitude towards edtech and the narrative created around them played a significant role in their success. The first element of this narrative is the idea that "education is broken". The second is the belief that Silicon Valley technologies were the solution (Weller, 2014). This narrative persists today, as briefly discussed in the introduction, and permeates the deployment of several other edtech. In 2021, the number of students enrolled in MOOCs reached 220 million (Shah, 2021).

101. After the MOOC trend, 2014 was marked by the peak of the discussion on learning analytics and the role of AI in education more broadly. The use of AI in education, with its automation capabilities based on associations, brings about a tremendous shift compared to traditional edtech. It not only captures data but also detects patterns within them and automates decision-making (Cardona; Rodríguez; Ishmael, 2023, p. 1).

102. These features can enhance educational services by improving the adaptivity of learning resources and supporting teachers' roles through automation. For instance, AI systems can draft curriculum and lesson plans, recommend content and help teachers develop tests. Educational chatbots help guide student learning, student admission and learning feedback (Hillman *et al.*, 2023). However, they also raise serious concerns regarding privacy and data protection, due to

their need to use large amounts of data, as well as their ethical and pedagogical implications. The automation feature of AI also promotes scalability, which means that the unintended or unexpected consequences can be direr (Cardona; Rodríguez; Ishmael, 2023, p. 3) and individualistic solutions can be shortsighted. Considering that AI capabilities permeate the main edtech adopted nowadays, these risks, mainly those related to children's privacy and data protection, will be unpacked in due time throughout the thesis.

103. Since the early 2000s, biometric technology—used for measuring a person's unique characteristics for identification purposes—has also been gradually introduced in schools worldwide. These characteristics include fingerprints, iris scans, voice patterns, behavior and more. Such data serve various purposes, such as enhancing school security, facilitating canteen payments, managing library borrowing, controlling door and locker access, enabling photocopying and access to computers etc. (Swist *et al.*, 2022). The use of biometrics in schools sparks a debate not only concerning the challenges posed by AI and datafication, but also regarding the necessity and proportionality of using very intrusive and surveillance technologies in education, especially when other forms of identification could suffice for the school's intended purposes (King; Persoon, 2022).

104. Around the mid to late 2010s, XR technologies became more accessible and affordable, thus being increasingly used for educational purposes. XR is a multimodal technology, which enables the merging of physical and digital realities. It includes augmented reality (AR), virtual reality (VR) and mixed reality (MR) (Cortesi *et al.*, 2021, p. 6).

105. The applicability of XR in education is still under-researched, but, according to Cortesi *et al.* (2021, p. 9–10), preliminary evidence suggests that XR could be potentially used in three main areas. First, XR technologies offer potential for skill-based learning, particularly in learning foreign languages, as immersion has shown to be beneficial for it. Second, XR can significantly broaden the range of hands-on learning experiences available to students, such as virtual journeys inside the human body. Lastly, XR provides new functionalities and opportunities for learners to engage in new ways that were previously not possible with other technological tools. It could be used, for example, in architecture classes to simulate designs.

106. Seen as the culmination or realization of the full potential of XR, as well as a way to solve some of the issues brought about by the COVID-19 pandemic, the metaverse is perceived as a technology that holds significant potential for education. Although the first attempts to introduce “virtual worlds” in education did not succeed around 2007, the metaverse discussions

came back with a vengeance after more than a decade, with even the company Facebook changing its name to “Meta” to mark this “new phase” of the internet—and also for rebranding purposes due to the controversies associated with its previous name (Isaac, 2021). Even nowadays, however, it can be said that society is still not technologically nor culturally ready for the metaverse. With the rising popularity of games such as Roblox, Minecraft and Pokemon Go, what we witness is a plurality of online worlds within a multiverse (Peckham, 2020) that represents the transition to the new digital frontier.

107. In education, metaverse-based learning promises to be more than the combination of in-person learning and screen-based remote learning. The main idea is to compensate for the limitations of both models (Zhang *et al.*, 2022), blending the analogue, online and augmented reality together for a seamless transition. However, the current state of the “multiverse” is still in the hands of a few companies. If education is to somehow profit from this new technology, it is crucial to start a discussion on public-service media and non-commercial zones in the metaverse, where under-served ideas, information and communities can flourish (Kleeman, 2021).

108. In 2020, the COVID-19 pandemic disrupted education around the world and every social interaction became digital by default. As described in this history, (digital) ICT have always played an important role in education, but the pandemic accelerated their implementation overnight. It indeed introduced new ways of learning, but also exacerbated existing inequalities, which prevented many children from fulfilling their right to education. Even when technology was easily accessible, technology-centered methods often resulted in low engagement and poor achievement (UNESCO, 2023a, 2023b, p. 12). It also aggravated the risks to children’s right to privacy and data protection, as they would use the digital environment not only for learning, but also for playing, and socially interacting.

109. With the limited historical distance currently available, we can view the COVID-19 pandemic as a prime illustration of the risks of technological solutionism and “challenge the assertion that educational technology investment necessarily strengthens education system resilience, and [...] that expenditure on education technology should necessarily scale up” (UNESCO, 2023b, p. 12).

110. At the end of 2022 and beginning of 2023, with the launch of ChatGPT, generative AI systems became extremely popular and have once again sparked discussions on the role of AI not only in education, but in society as a whole (Center for Democracy & Technology (CDT),

2023). The very concept of generative AI is still disputed, but one way of defining it is “a technology that (i) leverages deep learning models to (ii) generate human-like content (e.g., images, words) in response to (iii) complex and varied prompts (e.g., languages, instructions, questions)” (Lim *et al.*, 2023, p. 2). As a relatively new technology, the challenges and opportunities of its use are still being mapped, but attention has been especially given to discussions like plagiarism, the relevance and role of assessments, limitations in relation to current data, the spread of misinformation, and new skills that students and teachers will need to develop (Center for Democracy & Technology (CDT), 2023; Lim *et al.*, 2023; UNESCO, 2023b).

111. Looking ahead towards the future of edtech, in a rapidly evolving world, new technologies emerge at an ever-accelerating pace, and AI systems capabilities seem to be developing on a monthly basis. This emphasizes the need not only to understand the operation of each of these emerging technologies but also to determine what kind of education we envision and what schools should offer to enable students to navigate a future in which humans and machines will be intricately interconnected. Understanding education as a promoter of the vision of history as possibility, more important than ever, “[e]ducation systems need to return agency to learners and remind young people that we remain at the helm of technology. There is no predetermined course” (Giannini, 2023, p. 4).

1.2 Edtech typology

112. As the brief history outlined above demonstrates, a wide range of technologies has been applied to education. For the most part, they were not initially designed for this specific purpose, which gives rise to particular challenges related to children’s human rights. To systematize the discussion and gain a better understanding of edtech’s various applications, this section aims to present a possible typology of edtech. This typology will serve as the foundation for explaining the scope of this thesis and determining the technologies that will undergo a legal analysis.

113. This typology was developed through the clustering and adaptation of previous research, as in Fedders (2019), Holmes *et al.* (2019), Pangrazio, Selwyn and Cumbo (2022), and Holmes *et al.* (2022). Since the central topic of this thesis is understanding the risks associated with children’s rights to privacy and to the protection of personal data, the typology will focus on digital ICT. ICT are understood as

a diverse set of technological tools and resources used to transmit, store, create, share or exchange information. These technological tools and resources include computers, the Internet (websites, blogs and emails), live broadcasting technologies (radio, television and webcasting), recorded broadcasting technologies (podcasting, audio and video players, and storage devices) and telephony (fixed or mobile, satellite, visio/video-conferencing, etc.) (UNESCO Institute for Statistics (UIS), 2009, p. 120).

114. More specifically, this thesis will concentrate on data-driven digital ICT, which encompasses technologies that collect, analyze, and make decisions based on data. These processes can be carried out by traditional data analysis technologies (which heavily rely on humans), using statistical methods and other mathematical techniques to identify patterns, discover relationships and gain insights from data. However, more often than not, this has been done by AI, including symbolic AI techniques or, more commonly (and also more heavily dependent on data), ML techniques.

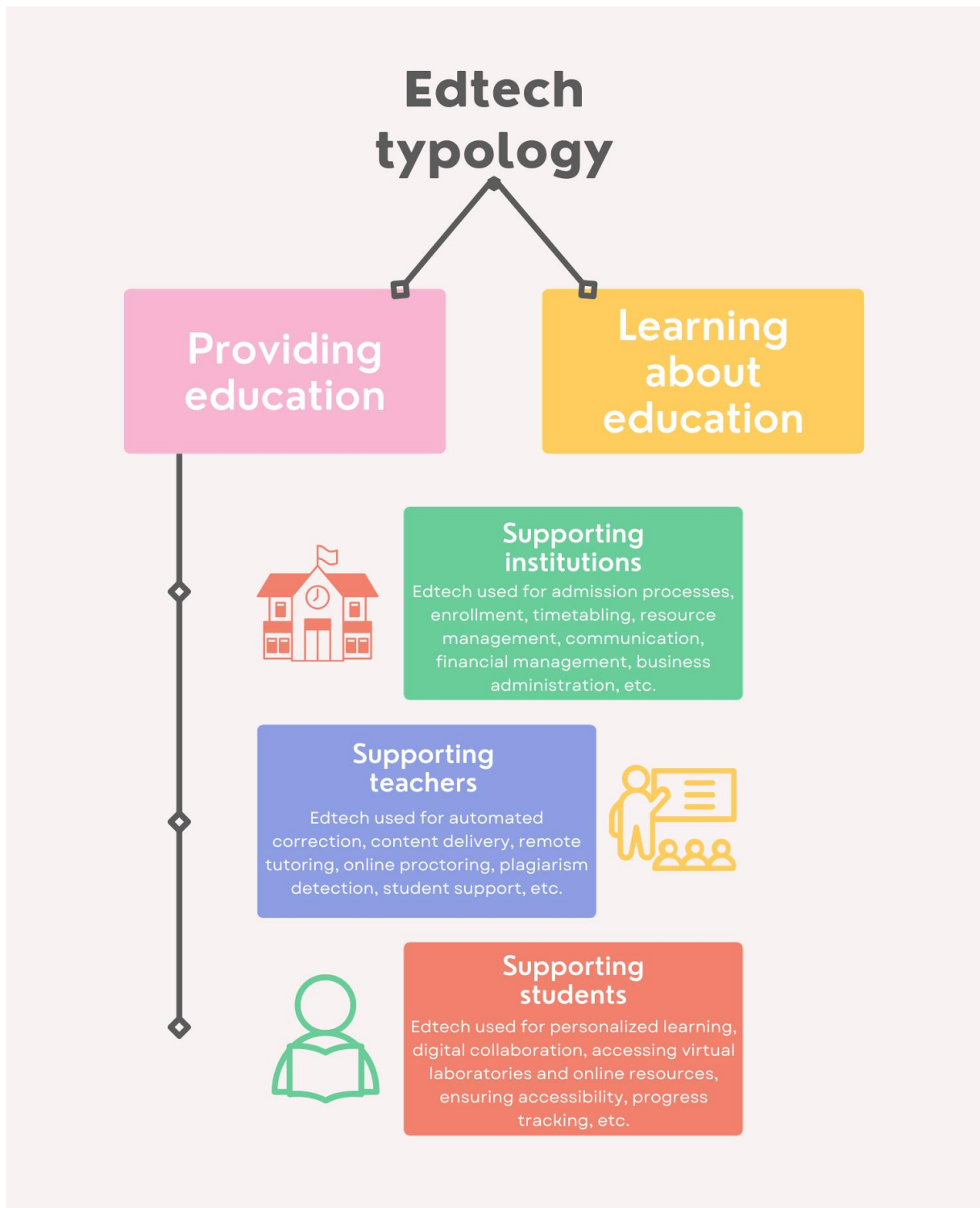
115. Defining AI is a very challenging task and there is no single definition that is universally accepted. For the purposes of this thesis, I will apply the definition provided by UNICEF. According to UNICEF (2021, p. 16), AI are

machine-based systems that can, given a set of human-defined objectives, make predictions, recommendations, or decisions that influence real or virtual environments. AI systems interact with us and act on our environment, either directly or indirectly. Often, they appear to operate autonomously, and can adapt their behavior by learning about the context.

116. This is a very interesting and functional definition. It incorporates various types of AI, and has a critical view of the role that humans play in their development and utilization (they depend on “human-defined objectives” and only “appear to operate autonomously”). However, this definition also has its drawbacks. One example is the application of the notion of learning to AI systems, which could be understood as something inherently human, dependent on agency and consciousness (Holmes *et al.*, 2022, p. 16). What machine learning algorithms actually do is essentially recognize patterns in the wealth of data they are fed with (Solove, 2024).

117. Based on these initial definitions, the typology can be presented. It is important to note, however, that the boundaries between each category are not always clear and the same technology can be used for different purposes and in different contexts. Especially when they are supposed to be a central hub or LMS, they will also often provide many options and possibilities to schools, educators and students, enabling it to feature in more than one category. The function of the typology is, therefore, to assist us in navigating this complex environment with a significant amount of available technology. Figure 1 provides a visualization of the typology.

Figure 1 - Edtech typology



118. The primary distinction that should be made is between the use of edtech for *providing education* and for *learning about education*. When it comes to *providing education*, technologies can be used, first, to support educational institutions. This includes supporting admission processes, managing student's and school's data, timetabling, managing resources

management, as well as facilitating communication among the school staff, students and parents/legal guardians. This encompasses processing data such as enrolment, attendance, grades, schedules, academic records, contact details, social media, human resources, business data and finances. Schools often use one or more platforms to help them manage these data. If understood more broadly, this category could also include parallel activities that use technology to support the institution. An example would be school security—whether physical or online—by applying video cameras (including the ones powered with facial recognition), iris detector, metal detector, turnstiles, etc.

119. Second, technology plays a crucial role in supporting teaching and learning. This includes a wide range of tools such as LMS, document creation applications, e-textbooks, online tutoring, e-proctoring systems, educational games, chatbots, and automated writing evaluation systems. These technologies can be more focused on students themselves, by automating teacher functions and promoting independent learning. They include personalized learning technologies, virtual laboratories, online resources, progress tracking tools, educational games, and chatbots. On the other hand, they can be designed to directly assist teachers by streamlining and automating tasks, such as automated correction, content delivery, remote tutoring, online proctoring, plagiarism detection, student support etc.

120. Most AI research in education has been developed with a focus on supporting students, often by taking over teacher-related tasks. In contrast, limited research has been conducted on AI systems designed explicitly to aid teachers instead of replacing them. Frequently, designers think of teachers only at the end of the process by adding, for example, a dashboard to the application (Miao *et al.*, 2021). However, the examples above highlight the flexible boundary between technologies that focus on students and the ones that focus on teachers (Holmes; Bialik; Fadel, 2019, p. 21).

121. Edtech could also be used for *learning about education*, commonly known as learning analytics or educational data mining within the AI field. This meta level encompasses collecting, analyzing, and interpreting data from edtech to understand and optimize learning and learning environments. In other words, the data collected during interactions between students, educators and the edtech platform is not only restricted to the initial purposes of the application but serves as a basis for uncovering patterns of how the learning process takes place. This generates new data that can be, eventually, fed back into the system to improve the algorithm or used for other purposes. This will be better detailed in the last part of the thesis.

122. Before moving to the second chapter, I would like to highlight that the above typology is just one way to cluster educational technologies and can certainly be complemented by other ones focusing on different aspects. It was based on who/what the technology supports, as well as their purposes, but it is also possible to group edtech based on the means through which it is presented to these stakeholders, for instance. The table below shows, within the global market share of edtech, examples of different ways edtech presents itself to the public, either as hardware, software or a service.

Table 1 - Examples of EdTech “products”, with % Global Market share (2019)

EdTech Hardware (9%)	EdTech Software (49%)	EdTech Services (42%)
Classroom Technology and Institutional Devices, including VR, XR, head-sets and other simulation devices.	Marketplaces, Peer to Peer Learning, Coaching and Mentoring Networks, Apps, Cloud-based management systems and tools.	All online forms of Primary and secondary education, higher education, tutoring and test preparation, online program managers and Bootcamps, as well as digital internships, apprenticeships and mentoring.

Source : Adapted from Vicentini *et al.* (2022, p. 16)

Interim conclusion

123. When tracing the historical evolution of edtech, we can perceive how diverse and rich its different applications are. We must look at this past not merely as steps leading us to the use of computers and AI in education, but as decisions made by humans that provide insights into how we can understand and regulate current technologies. Many of these technologies were not designed with education or children in mind, which can pose extra challenges to children’s rights.

124. As we will see in the upcoming chapters, the education measurement movement, along with behaviorism, which played significant roles throughout the 20th century and shaped the development of early teaching machines, continue to influence current edtech. Therefore, reflecting on the past and the technologies that preceded those we use today also helps us understand enduring patterns and learn from previous experiences.

125. Setting the stage for the legal analysis, I have also introduced a typology of edtech that guides us through the complexity and great amount of edtech currently available to educators.

As in any categorization of complex phenomena of reality, the boundaries between the categories are blurred. Nevertheless, it can still be workable and helpful in identifying and systematizing the impacts that technologies have on the privacy and data protection of children. This typology will be used in the final part of the thesis when risks related to edtech to these rights will be mapped.

Chapter 2. Exploring the interplay between edtech and longstanding discussions in education

126. The proliferation of edtech, especially the introduction of digital ICT in education, has sparked a dynamic interaction between educational developments and the imperatives and constraints introduced by technology. On the one hand, edtech is imbued with specific design features that either enhance or limit certain actions and pedagogical methodologies. On the other hand, they were not introduced in a vacuum nor applied to blank slates, as education was already undergoing significant changes that benefit or face challenges in adapting to technology. As previously discussed, education is an inherently political and contested domain that encompasses various strands of theory and practice, each interacting with technology in unique ways.

127. This chapter will thus seek to present some of the main issues that arise from this mutual influence. This includes enduring questions such as the role of private actors in education, the demand for “efficiency,” and the learnification of education phenomenon, as well as more contemporary issues, such as the concept of platform learning. Each of them represents a crucial dimension shaping the present and future trajectory of education, raising significant issues about its nature, its role in society and how technology interferes with it. This chapter is important for gaining a broader and more holistic understanding of the risks that technologies can pose to children’s privacy and data protection. Some of the trends analyzed here may either curb or encourage certain technological features, affecting these rights to varying degrees.

2.1 Public and private values in education

128. Public institutions are foundations of western societies and some sectors, such as education, are considered public or common goods (UNESCO, 2015), essential for the maintenance of the rule of law, democracy, and human rights. Education is crucial to equip individuals to make informed decisions within a community, enable civic participation; foster tolerance and diversity, as well as promote social and economic development.

129. Public education can actually be considered as a matter of international human rights law. The structure of the rights within the CRC and the International Covenant on Economic, Social and Cultural Rights (ICESCR) is such that they first lay down the right to education (as well as the general principles that should be sought in order to fulfil it), only then to recognize

a right for individuals to establish and attend schools other than public ones. The scheme and the wording of these provisions would prioritize education provided by states as the “norm” (Mowbray, 2021).

130. We can also argue that public education is the best form of democratic education. Heimans *et al.* (2022, p. 71) is of the view that “what is ‘public’ about public education emerges from when democracy is put into practice *in* education”. Democracy here is focused not only on the system’s features (such as voting, political representation etc.), but on democratic acts or moments. When people engage in these acts and moments and become part of them, especially those who were previously excluded from the sense-making process, it can be said that education “becomes public” (Heimans; Singh; Kwok, 2022). According to the authors, this kind of education would be at odds with efforts of standardization and the perception of education as a product that could be exchanged in the market.

131. However, with the globally growth of neoliberal policies in the 1980s, the public sector started to be depicted as unproductive in comparison with the private sector, leading to the worldwide implementation of policies limiting public expenditure. This phenomenon has fostered the *marketization* of education, i.e., the “creation of a series of policy logics that aim to create quasi-markets in education” (Hogan; Thompson, 2021, p. 3). This was especially reinforced by the education sector strategies encouraged by the World Bank in developing countries (Singh, 2015a).

132. This means that private actors are increasingly involved in a service that was once mainly provided by the state. While the relationship between public and private entities in education has always existed (consider, for instance, the commercialization of textbooks), this has intensified (Hogan; Thompson, 2021), resulting in an environment characterized by “power-sharing, negotiation and competition, where decisions are made through a complex web of network interactions” (Castells, 2010, as cited in Hogan; Thompson, 2021, p. 3). It also implies that the service is more focused on individual needs, rather than on the common good, potentially fostering discrimination, and hampering equality of opportunities and social justice (Singh, 2015a).

133. The marketization of education can be realized in two forms: privatization and commercialization.

Privatization is the development of quasi-markets through institutional and policy structures that privilege parental choice, school autonomy and venture philanthropy, often with the state regulating for public accountability. It happens *to* schools. [... On the other hand], [c]ommercialization is the creation, marketing and sale of education

goods and services for commercial gain. It happens *in* schools. [...] While privatization is about the logics of who conducts education, commercialization is about how actors profit from the “commodification” of education (Hogan; Thompson, 2021, p. 3, emphasis in the original).

134. The school influenced by neoliberal policies is then related to understanding education as an essentially private good, whose value is, above all, economic. According to this narrative, education should not necessarily be provided by society, or the government, but should be mainly the product of the investment of individuals. The notion of the full autonomy of individuals with no strings attached, except those they themselves recognize by their own will, corresponds to institutions focused on serving particular interests, transforming citizens into clients (Laval, 2019, p. 17).

135. The reduced involvement of the government, the marketization phenomenon, and the responsabilisation of individuals through economics compel people to make risky choices about every aspect of their lives, including education. Peters (2005, p. 131) explains that “[c]hoice” assumes a much wider role under neoliberalism: it is not simply ‘consumer sovereignty’ but rather a moralization and responsabilisation, a regulated transfer of choice-making responsibility from the state to the individual in the social market”. If individuals are to bear the responsibility and possibly the costs of education, that also means that providing several market options would be the best strategy to improve competition and diversification in the service provided (Lubienski, 2021, p. 22).

136. This not only places the burden on individuals, who do not necessarily have all the information and bargaining power to make a decision suited to their best interests, but is also corrosive to democracy. A “consumer-based public sector is limited in its ability to address the perverse effects of choices and to build stable and reliable institutions” (Needham, 2003, as cited in Peters, 2005, p. 135–136). If, on the other hand, the provision of education is focused on its collective benefits, then the emphasis should be on “issues of access and adequacy, equity of outcomes and guaranteeing that all students have quality schools—issues often better addressed by public governance or direct state provision” (Lubienski, 2021, p. 22).

137. The dynamics of the private sector are introduced in the public sector primarily under the efficiency argument, which will be further elucidated in Section 2.3. This is brought about by reducing public investment in education: more needs to be done with a smaller budget, and management techniques that have already been put to the test in the private sector start to be incorporated (Laval, 2019, p. 193). When it comes to edtech, the role that private actors have on taking important decisions in education also increases, ranging from determining (part of)

the content that is learned, to defining pedagogical strategies and interpreting a child's educational development (Knox, 2020).

138. Edtech wields immense influence over contemporary childhood education, shaping what can and cannot exist, setting priorities, and fundamentally defining its nature based on the investors backing edtech companies. Edtech made education *investable*, which means that more than financial decisions, investors make political decisions that affect the whole society (Komljenovic *et al.*, 2023). As one edtech investor puts it, the most difficult part in investing in innovation is “[w]hich new ideas will work? Which new ideas will be purchased—at what unit price and what gross margin? Which new ideas will scale and deliver consistent and increasing revenue, ROI [Return of Investment] and profitability? [...]” (Palmer, 2022, n.p.).

2.1.1 The role of philanthropy in education

139. The role of philanthropy also contributes to the privatization and commercialization phenomena. This is of course not a new event, but “the new generation of impact or ‘venture philanthropy’ often treats giving as an investment that needs to be strategically managed for maximum effectiveness and return” (Saltman, 2010, as cited in Lubienski, 2021, p. 23).

140. Important examples include the Gates Foundation, Dell Foundation and Chan-Zuckerberg Initiative, all of them related to technology companies. Although they are very much relevant in the USA, they already have a lot of influence in the whole world. These institutions embrace varied agendas, but they converge in transforming schools through top-down market models and business approaches, funding institutions and individuals, and defending advocacy strategies in public policy (Lubienski, 2021, p. 24).

141. The emphasis on individual purposes present in philanthropist agendas has severe implications for the governance of education, as the methodologies and remedies used to tackle educational problems will be defined by their interests. After analyzing the “social divisions”⁹ within some big tech companies, Magalhães and Couldry (2021) argue that these companies understand social good as being datafied, probabilistic and profitable.

142. By datafied, the authors mean that “social good is generally taken as proportional to and made comprehensible by the quantity, type, and granularity of the data that can be gathered”

⁹ By this, the authors mean “more or less organized sectors within Google, Facebook, Amazon, Microsoft, and IBM that define themselves as geared toward helping (typically, vulnerable) people, not profit” (Magalhães; Couldry, 2021, p. 347).

(Magalhães; Couldry, 2021, p. 349). The lack of data is generally seen as a barrier that impedes social good to be realized and the investment and tools provided by big tech as the solution. This is also related to the fact that data about humanity in general is increasingly held in private hands.

143. The datafication of social good leads to the idea of probabilistic good, as the attempt to make sense of data is related to a language of probability. The problem with this approach is that “the association between (probably) doing good and (necessarily) allowing some harm to happen flows automatically from the probabilistic notion of algorithmic knowledge on which proponents of datafied social good choose to rely, as their model for producing social knowledge” (Magalhães; Couldry, 2021, p. 352).

144. Finally, the projects conducted by these social divisions seem to be inseparable from profit generation, as datafication can hardly be separated from commodification (Dijck; Poell; Waal, 2018, p. 121). This happens not only because of their role in big tech’s marketing strategies, but also because they are entangled with their commercial products (Magalhães; Couldry, 2021). As will be further discussed in Part III of this thesis, Google Workspace for Education serves as a prime example of this model. Although mostly offered at no cost, it concurrently collects vast amounts of data from students, which may potentially be leveraged for commercial purposes.

145. This kind of philanthropy is often driven by the idea of disrupting sectors, such as education, but it also “tends not to act in ways that are counter to the interests of the wealthy, nor to ‘disrupt’ the systems or exploitative practices that produced the vast fortunes that these philanthropists now leverage” (Lubienski, 2021, p. 30). It also raises the question of the origin of the money employed by these organizations, as they are often linked to predatory business practices (Lubienski, 2021).

146. The digital transformation in public sectors such as education (partially) funded by the private sector is often seen as very attractive and benign (Alston, 2019, p. 4). However, beyond the challenge of estimating the effects of this influence on education¹⁰, if imbued with strong individualistic and private values, it can also be viewed as a “Trojan Horse for neoliberal hostility towards welfare and regulation”, as described by the former UN Special Rapporteur on extreme poverty and human rights, Philip Alston (2019, p. 12). This has a significant impact

¹⁰ See, for example, Strauss (2013) and Hess (2020).

on countries that do not have large-scale data actors, robust systems for data processing, and have limited connectivity infrastructure (Magalhães; Couldry, 2021, p. 346).

2.2 The “learnification” of education

147. According to Biesta (2010), the last decades have seen the intensification of a phenomenon called the *learnification* of education. This means that the discourse around education has been translated into a discourse of learning, i.e., a narrative that focuses solely on the knowledge and skills that should be acquired by individuals. Teaching is seen as an activity that supports or facilitates learning (Biesta, 2016a, p. 15).

148. This results from a confluence of events rather than the intended outcome of a particular agenda. The author highlights four main trends contributing to it: a) emerging theories of learning, especially constructivist and sociocultural theories, which challenge the idea that learning is a passive exercise and advocate for the active construction of knowledge by learners; b) postmodernism, which understands education as a project of modernity, intimately connected with the Enlightenment. It casts doubt on the idea that education can emancipate students through rationality and critical thinking; c) the silent explosion of adult learning, and the fact that people spend increasingly amounts of time and resources on learning both within and outside established educational institutions; and d) the erosion of the Welfare State; While neoliberalism’s market-oriented ideology has not entirely supplanted the principles of the Welfare State, such as universal education, the dynamics of citizen-government relations have shifted. Instead of a political relationship, it is increasingly an economic relationship, where the state is seen as a provider of public services and the taxpayer as a consumer (Biesta, 2016a, p. 17–19).

149. The main issue related to this language is that it, deliberately or not, promotes the idea of education as an economic transaction, where the learner has needs that the educator should fulfil. Ultimately, education becomes a “thing”, a commodity that can be consumed by the learner (Biesta, 2016a, p. 19–20), which is related to the issue of private actors in education as discussed above.

This is the logic that lies behind the idea that educational institutions and individual educators should be flexible, that they should respond to the needs of the learners, that they should give their learners value for money, and perhaps even that they should operate on the principle that the learner/customer is always right (Biesta, 2016a, p. 20).

150. It assumes that children and their parents or legal guardians know exactly and in detail what they want from school. This assumption fails to consider that one of the primary objectives of pursuing education is to determine one's actual needs, and this process heavily relies on the involvement of educational professionals with the necessary expertise (Biesta, 2005, p. 59). That is exactly the difference between a market model and a professional model, which lies in the latter's emphasis on producers not just servicing a need, but also helping define it (Feinberg, 2001, p. 403, as cited in Biesta, 2005, p. 59).

151. The learnification phenomenon is also aligned with understanding education as the provision of human capital for the economy (Holmes *et al.*, 2022, p. 27). This human capital should be qualified and skilled and, therefore, the focus of education should be on the content that children are receiving.

152. It is important to highlight that this new language is not problematic *per se* and can even empower individuals to take control of their educational agendas. It could also help redress imbalances created by inflexible and provider-led situations, excluding many from educational opportunities (Biesta, 2016a). However, the language we use to describe the world directly influences reality and set the boundaries of what is possible to be said, to know, to be thought and, ultimately, to be done (Biesta, 2005, p. 54).

153. Framing education as purely learning reduces its scope and reach. It focuses only on the qualification aspect of education (related to acquiring knowledge, skills, values etc.), and sidelines the aspects of socialization ("the ways in which, through education, we become part of existing traditions and ways of doing and being") and of subjectification (related to the subjectivity or "subject-ness" of the educated, raising questions related to emancipation and freedom) (Biesta, 2016b, p. 4). The "learnification model is predicated on the real-time, short-term process of learning, while education involves a simultaneous nourishing of intellectual, social, technical, and cognitive skills and involves a longer trajectory over a period of years" (Dijck; Poell; Waal, 2018, p. 124).

154. If the problems stem from inequality and limited access to education, the priority should be addressing the root cause, rather than confining education solely to learning outcomes. We should be focusing on making education, broadly understood, more human and democratic, ensuring that all individuals, including children, actively participate in decisions that impact them. Moreover, education should not only be seen as an individual path or preference, but also as a way for students to become citizens and active political actors.

2.3 Learning, calculation and efficiency

155. The narrow focus on learning, as explained above, is open-ended in relation to the objectives of education. Judgements in education should, however, not only be related to what is possible (factual judgement), but also what is desirable (value judgement) (Biesta, 2010, p. 37). Learnification deflates a collective and democratic discussion about the reasons and ends of education beyond individual preferences, diverting attention to procedural aspects. Consequently, questions tend to gravitate towards technicalities and efficiency.

156. A framework that is only focused on the means is never neutral. The efficiency of teaching in the way it develops in neoliberalism tends to be confused with economic efficiency, which consists of maximizing countable results (Laval, 2019, p. 213). The idea of effective intervention (a causal model between the intervention and the results), that was first developed in medicine, comes from a particular understanding of professional practice that is not necessarily well translated to education (Biesta, 2010).

157. Education, however, is not a physical interaction, but rather a symbolic or symbolically mediated interaction. “If teaching is to have any effect on learning, it is because of the fact that students interpret and try to make sense of what they are being taught. It is only through processes of (mutual) interpretation that education is possible” (Biesta, 2010, p. 34). What teachers do (and here it is also possible to include any other input that the student receive) should be than seen not as the cause of learning, but as an chances “for students to respond and, through their response, to learn something from these opportunities” (Biesta, 2010, p. 35).

158. The demand for efficiency is intrinsically related to the measurement of education and, consequently, to datafication (Barassi, 2020, p. 72). The rise of the measurement culture in education dates from the 20th century, when large-scale assessments that trace performance and growth even across borders started being applied to drive evidence-based decision-making (Pangrazio *et al.*, 2022, p. 259–260). In 1904, one of the main proponents of the idea of measuring education was the American psychologist Thorndike, who believed that units of measurement should be devised, tested and standardized in education so the latter could yield the true benefits of quantitative science (Lawn, 2013, p. 110).

159. This process was extremely important so decisions in the educational realm started to be informed by factual data, rather than by mere opinions of what education should be. However, the excitement with the abundance of information has also resulted in an exacerbated

reliance on factual data (Laet *et al.*, 2018). Measuring not only refers to a new way of describing education, but a new definition of education and the relations within it (Lawn, 2013, p. 110). With the measuring movement, not only students are analyzed; schools are also assessed in order to check whether they meet national goals and have their data scores ranked against each other (Barassi, 2020, p. 74). Children become proxies for school performance, while schools become data centers (Williamson, as cited in Barassi, 2020, p. 75).

160. Computing language helps compartmentalizing and calculating learning and achievements. It reframes and explains educational dynamics, proposing that education can be programed, executed and standardized. More than that, it starts to delineate what counts as knowledge or not.

[P]eople begin to think that socio-cultural processes could be engineered, streamlined and automated (i.e. orchestrated) to enhance performance and efficiency. In some cases this becomes more than a simple belief, as it begins to constrain practices by imposing a technocratic ideal of how education should be run (Perrotta; Evans, 2013, p. 522).

161. Quantitative data concerning educational outcomes is undeniably useful. However, a genuinely scientific spirit should question the limits of these assessments, the uses that can be made of them and the practical consequences they can have, especially in the pedagogical field (Laval, 2019, p. 214). More than questioning if one is measuring what they want to measure, the problem lies in the normative validity of the measurement. That is related to the question

whether we are indeed measuring what we value, or whether we are just measuring what we can easily measure and thus end up valuing what we (can) measure. The rise of a culture of performativity in education—a culture in which means become ends in themselves so that targets and indicators of quality become mistaken for quality itself—has been one of the main drivers of an approach to measurement in which normative validity is being replaced by technical validity (Biesta, 2010, p. 13).

162. This is related to what Laval (2019, p. 16) calls the cult of “innovation” for the sake of “innovation”, which is dissociated from clear political implications. The discussions about edtech should then be focused not on the technology itself, but on the educational challenges we as a society would like to tackle, such as equity and inclusion, as well as education’s quality (UNESCO, 2023b, p. 7). Efficiency and the tools we choose to use are also a very important part of the discussion, but they should be focused on *supporting* the achievement of these broader goals.

2.4 Platform learning

163. The way the digital economy is currently constructed heavily relies on platforms and they are one of the main data infrastructures present in schools. Platforms are a “programmable digital architecture designed to organize interactions between users [... and are] geared toward the systematic collection, algorithmic processing, circulation, and monetization of user data” (Dijck; Poell; Waal, 2018, p. 4). They are increasingly the way through which education takes place in the digital environment, especially from 2010 onwards (Rivas, 2021).

164. It is important to remember that a platform is always a means to something else. While platforms are often assessed based on their functionality, such as the delivery of goods and services, it is crucial to examine the manner in which they operate, specifically how they facilitate interactions between users, service providers, and other technical systems (Nichols; Garcia, 2022, p. 213).

165. Van Dijck (2013) understands platforms as a metaphorical construct with technological, social, economic and political dimensions. These dimensions coexist and influence one another, meaning that all of them should be assessed when deciding if and which platform will be used within an educational setting. Platforms should also not be understood as static tools, but as having a living and dynamic nature, which the author compares to a tree. They are constantly evolving and shaping their environment and they are part of a larger global connective network (Dijck, 2021, p. 2805).

166. Within the school environment, platforms significantly shape students’ and teachers’ social experiences, as well as how data are processed within its architecture. They differ from previous software solutions in that they not only provide services to their users, but also collect data from these interactions, which their owners can sell or use for product development (Nichols; Garcia, 2022, p. 210). The interfaces users interact with change in real time based on these data and it learns from users’ behavior, which makes them unique to each user (Susser; Roessler; Nissenbaum, 2019, p. 7). In this sense, while education datafication provides platforms with the data for analytics, platforms are essential for collecting, structuring and representing them (Pangrazio; Selwyn; Cumbo, 2022, p. 2).

167. As an entry point for making sense of data, platforms “help concretize otherwise abstract data processes by locating them in particular socio-technical and political-economic relations” (Pangrazio *et al.*, 2022, p. 261). Being rooted in the *learnification* narrative, they are “imagined

as a customizable on-demand service as learners interact with platforms like users interact with Netflix, Facebook, Amazon, and iTunes” (Means, 2018, p. 329). In fact, to become “the Netflix of Education” was exactly Pearson’s (a British multinational publishing and education company) goal (High, 2018).

168. When this model is applied to education, it “reflects a belief in learning as a prescriptive process, rooted in efficiency and calculation, and powered by artificial intelligence, mobile apps, cloud services, and data processing” (Means, 2018, p. 329). Thus, they are the perfect way to implement the efficiency and evaluation culture described in the previous subsections and their design is often shaped to transform social interactions into data and quantifiable knowledge.

169. It is important to consider that over time, humans often become accustomed to using technology, focusing primarily on the tasks it facilitates rather than on the technological means itself. Consequently, because technological tools can fade into the background, their influence might go unnoticed, potentially allowing for hidden and manipulative practices to persist (Susser; Roessler; Nissenbaum, 2019, p. 7). Therefore, learning powered by platforms can uproot or bypass the core values of publicly funded education, such as a knowledge-based curriculum, teacher autonomy, affordability, and education as a means for socioeconomic equality (Dijck; Poell; Waal, 2018, p. 118).

170. The main platform usually used within the school is the LMS, and it is part of the broader data infrastructure, which also includes human and material infrastructure such as cables, routers and servers (Pangrazio; Selwyn; Cumbo, 2022, p. 4). LMS are designed to provide a centralized platform for managing and delivering educational content, activities, and assessments. They usually support a wide variety of teaching and learning modalities and integrate with other more specific applications. This implies that the possible activities that can be carried out within a LMS are diverse, encompassing content management, communication, discussion forums, online quizzes, and assignment submission. This also means that they can serve as central hubs for data collection. This underscores the significance of examining Google Workspace for Education as an LMS in Part III, as it provides interesting insights into the challenges related to children’s rights to privacy and to the protection of personal data while using edtech.

Interim conclusion

171. This chapter aimed at unraveling the complexities arising from the intersection of long-standing questions within education and the influence of edtech, with their inherent promises and limitations. I have argued that public education is the best way not only to implement, but also to promote democracy in our society, as well as to nurture critical and informed citizens. When education is treated as a private good and citizens are cast merely as consumers, the focus narrows down to individualized needs, overshadowing its broader societal role and neglecting other collective values. I have also discussed how neoliberal educational policies are one of the reasons behind the phenomenon of “learnification” of education, prioritizing individual knowledge and skill acquisition. While this shift can empower individuals in their educational agendas, it risks minimizing the significance of education, overlooking crucial aspects of socialization and personal development.

172. Understanding education solely as learning also seems appealing as it reduces its qualitative aspects. The more quantifiable education is, the easier it is to measure it and, therefore, focus on efficiency. The growing emphasis on efficiency tends to prioritize its economic aspect over the symbolic interactions fundamental to the educational process. Despite this measurement culture having roots in the early 20th century, the advent of data-driven digital ICT has intensified this trend through datafication.

173. The use of edtech interacts with these trends by facilitating the involvement of private actors in education, given the increasing use of technology in the field, and by enabling interaction among students, educators, and companies within platforms. The implementation of platforms aligns with the trend of the learnification of education and the measurement movement, which remains strongly present today. They facilitate user interactions and data collection, having progressively become the primary mode of education delivery. They are more than mere functional tools; their dynamic nature shapes social, economic, and political dimensions and reflect an efficiency-driven, data-centric narrative, akin to consumer platforms like Netflix. This model risks undermining core educational values and reinforcing inequalities.

174. In light of these developments, technology should be seen as a valuable tool in education, with the potential of enhancing learning and even other aspects of education such as socialization and subjectification. However, the focus should not be on innovation for its own sake but rather on leveraging technology as part of a comprehensive strategy aimed at achieving educational goals like equity, inclusion, educational quality, and children’s best interests.

Chapter 3. Data Colonialism as a theoretical and normative framework

175. Within legal scholarship, research frequently entails a summary of the current state of positive law, combining reference to legal sources, such as legislation and cases, with the analytical doctrine. However, less frequently identified is the explanation of how researchers, through this review of the current state of the art, reach conclusions and normative claims (Taekema, 2018). A theoretical framework becomes essential to shed light on the lens that the researcher adopts to see the social reality. It not only enhances transparency but also aids the reader in understanding the reasoning that leads the researcher to their conclusions, making research reproducible.

176. Considering that the majority of legal research is not only descriptive or explanatory but also normative, the theory also needs to serve as a normative framework. It provides the link to prior research and the foundation for an evaluation of the current affairs and/or proposing a solution (Taekema, 2018).

177. Therefore, as a theoretical and normative framework, this research adopts data colonialism, as described by Couldry and Mejias (2019). This normative framework will help evaluate the current state of positive law to answer the research question in the last part of this thesis. This chapter unpacks this framework and complements it with a broader literature on datafication and data colonialism that can help clarify some of the concepts developed in the book. Apart from explaining what data colonialism is, its main components, and the actors involved, I will also focus on how it disproportionately affects some people and communities, as well as how it is rooted in very specific business models. Finally, I will discuss the implications of data colonialism on human autonomy.

3.1 The concept of data colonialism

178. The concept of data colonialism, as developed by Couldry and Mejias (2019, p. xiii, xix), refers to an emerging order of appropriation of human life through data. The authors do not use the term colonialism as a metaphor, but as a concept that encompasses significant evolutionary stages throughout human history, with a particular focus on the context of capitalism. It does not mean, though, that there is a one-to-one correspondence between what is happening within data colonialism and the highly violent activities of historical colonialism.

179. This is because colonialism's core is not understood as a particular method since they can be complex and varied (including not only physical violence but also symbolic forms of violence through legal, social and technological constructs). It is actually understood as a universalist view of the world's economic and cognitive resources (Couldry; Mejias, 2023, p. 794). While historical colonialism was focused mainly on natural resources and human labor, data colonialism adds a layer of human relations captured through data.

180. The data colonialism theory refers to the exploitation of human life and social relationships by a few entities through datafication and data commodification. It stresses that data do not naturally exist by themselves as if they were a natural resource. People do not "leave behind" digital traces or footprints as they wander around the digital realm; rather it is technology that facilitates the collection of these data. Data are always the outcome of an abstraction process, which transforms the whole of social life and meaning into something that can be counted. If it cannot be measured and counted, it does not exist (Mejias; Couldry, 2019, p. 3–4). It thus implies selection and transformation of reality which can be said to be a biased way to interpret and represent the world.

181. The datafication of human relations leads to the progressive reconfiguration of larger parts of the social domain, in ways that position technology companies as privileged providers not only of social solutions, but also of social knowledge (Magalhães; Couldry, 2021, p. 354). This is possible due to *data relations*, which is a new type of social form. They ensure that the collection of personal data and their storage give rise to a new type of knowledge about the social world: the so-called *social caching* (Couldry; Mejias, 2019, p. xiii). In many cases, this is a relation that has to be built to implement the data flow since data extractability only exists because it is socially constructed (Couldry; Mejias, 2019, p. 27).

182. Important for this thesis is the fact that targeting vulnerable social groups is considered by the authors to be an important part of data colonialism (Couldry and Mejias, 2019, p. 67–68, 148–149). Although every person's data would contribute as an input to data colonialism, some people at the margins of the social and economic order would pay a higher price. This includes not only people within the Global South, for example, but also children and other vulnerable data subjects even within the Global North.

3.2 Main components of data colonialism

183. In order to better understand the idea of data colonialism, the authors propose four main components that can be identified in both data colonialism and historical colonialism (and for that very reason, it is possible to recognize the historical continuity between one and the other). It is important to note, however, that the world has undergone fundamental changes over the past centuries, which provided data colonialism with some particularities. Without globalization, financialization, the acceleration of capital flows, as well as the huge development of communication infrastructures, the current way of processing data would not be possible (Couldry & Mejias, 2019, pp. xii, xix).

184. This highlights the relationship between the development of industrial capitalism and data colonialism. Couldry and Mejias (2019, p. xix) argue that the latter is driven by the imperatives of the first, which includes the logic of accumulation, profit maximization, competition, labor productivity through the technological elaboration of production, as well as growth through the reinvestment of surplus (Zuboff, 2019).

185. On the other hand, “capitalism itself emerged on the basis of colonialism’s detailed histories, in particular the European colonial power’s vast aggregation of global resources that fueled industrial capitalism”¹¹ (Couldry; Mejias, 2023, p. 787). Data colonialism is then the link that emphasizes how the relations between colonialism and capitalism are contemporary and evolving. This correlation is exacerbated by the current convergence of economic power (generating value) and cognitive power (generating knowledge) since data colonialism is appropriating the very resources for knowing the world (Couldry & Mejias, 2019, xii).

186. The first component is the *appropriation of resources*. Whereas historical colonialism was embedded in the *terra nullius* legal doctrine (the idea that some lands belonged to no one), in data colonialism, data are assumed to be there for the taking as a freely available resource (Cohen, 2019, p. 48; Couldry; Mejias, 2019, p. 88). Datafication is key for the processes of

¹¹ Neocolonial legacy still shapes capitalism’s development, as can be exemplified by Facebook’s Free Basics program (Facebook, [s. d.]). Cohen (Cohen, 2019, p. 59) describes the patterns in exploration and colonization of the public domain in two steps: “initial extensions of surveillance via a two-pronged strategy of policing and development, followed by a step back as the data harvests are consolidated and absorbed”. However, more than facilitated by historical colonialism’s current influence on societal and economic relations, extracting value through data would be a new form of resource appropriation, starting a “new stage of colonialism that lays the foundations for new developments in capitalism” (Couldry; Mejias, 2023, p. 788). Understanding this new form of life appropriation for profit only under capitalism, as does Zuboff (2019), for example, misses the point of the “Big Data rhetoric which insist [sic] that only through maximal collection and concentration of data can the world be developed, understood, governed, and saved” (Couldry; Mejias, 2023, p. 796).

commodification and privatization of data, which means that data (and, more specifically, big data) are being produced not only with its use in mind but also with the explicit purpose of market exchange (Couldry; Mejias, 2019; Thatcher *et al.*, 2016).

187. The second component is the *unequal social and economic relations* that secure resource appropriation. The historical colonialism framework included moral or legal norms that would allow forced labor, for example. Within data colonialism, what the authors call “data relations” makes the appropriation of human beings’ data seem normal and it is generally enforced by the technology design itself, as well as legal frameworks (Couldry; Mejias, 2019).

188. These data relations, especially between the colonizing agents and data subjects, are asymmetrical due to how obscure the transformation from individual data points to big data is (Thatcher; O’Sullivan; Mahmoudi, 2016). They provide corporations with a privileged overview of social relations, which is incredibly powerful. States are ever more dependent on this knowledge, reversing the longstanding flow of knowledge transfer (Couldry; Mejias, 2019, p. 13).

189. The third component is the massively *unequal global distribution of the benefits of resource appropriation*. While historical colonialism would concentrate wealth in colonizing nations, data colonialism favors the concentration of wealth in the hands of the colonizing agents (Couldry; Mejias, 2019).

190. As explained above, the control of data collection processes provides a special power to those who own the hardware and software that process them. As it stands, the “data economy” tends to be monopolistic, reinforcing other asymmetric balances of power (Cheng, 2020). This monopolization is not only restricted to services; being also present in the production of devices through which people connect to the infrastructures of data collection, in the computer capacity, production of content, and content delivery (Couldry; Mejias, 2019).

191. Finally, the fourth component is the spread of *ideologies that help make sense of the new order*. Within the historical colonialism framework, it was common to reframe “colonial appropriation as the release of ‘natural’ resources, the government of ‘inferior’ peoples, and the bringing of ‘civilization’ to the world” (Couldry & Mejias, 2019, p. 4).

192. Data colonialism, on the other hand, is embedded in several ideologies, such as, for example, the ideology of connection, which naturalizes the connection between people, objects and processes through computer-based infrastructures. “Connection is, of course, a basic human value, but the requirement to connect here and now—connect to this particular deeply unequal

infrastructure—means submission to very particular conditions and terms of power” (Couldry; Mejias, 2019, p. 16).

193. The authors also mention the ideology of datafication—which perceives that all aspects of human life can and should be transformed into data—and the ideology of personalization—which makes surveillance attractive. In a similar vein, Van Dijck (2014, p. 198) describes *dataism* as the “belief in the objective quantification and potential tracking of all kinds of human behavior and sociality through online media technologies”.

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

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

195. This mainly occurs because of the asymmetrical extraction of value through datafication, which assumes that quantification and surveillance of all aspects of human life are natural and desired by all members of society (Thatcher; O’Sullivan; Mahmoudi, 2016, p. 991). This myth empowers technologies and can undermine human autonomy.

3.3 Colonizing agents

196. The network of actors participating in data colonialism is a complex one. The result of data colonialism, i.e., what the authors call the “cloud empire”, is being implemented and extended primarily by the “social quantification sector”, the industry sector devoted to the development of the infrastructure required for data collection (Couldry & Mejias, 2019, p. xiii).

197. The social quantification sector is composed not only of the most obvious players, such as the Big 5 (Amazon, Apple, Google, Facebook and Microsoft). It also includes smart appliances manufacturers, developers of digital environments, data brokers, financial companies, and data-driven platforms (such as Netflix, Spotify, Airbnb and Uber) (Couldry & Mejias, 2019, p. xiv).

198. Although not at the center of the data colonialism process, other businesses were also transformed to accommodate data colonialism into society’s life. Ordinary businesses increasingly not only collect data for their internal purposes, often sharing them with other

actors, but also depend on the social quantification sector for services such as targeting advertisement and data storage (Couldry & Mejias, 2019, p. xv).

199. At the same time, the activities of the social quantification sector do not flourish without the active participation of states, which allows (or at least do not regulate) certain social relations. Knowing the social world in depth was previously just a prerogative of the State. Currently, it is the large technology companies that have this privilege, and states have become progressively dependent on them.

3.4 Data Commodification

200. One of the main conditions for the existence of data colonialism is understanding data as a commodity, i.e., something that can be traded in the market. Once collected and analyzed, data can be sold as a product or service in the digital economy. It does not mean that an ownership right is required. The data flow paradigm which reinforces commodification can be identified even when the legal framework recognizes *data access obligations* as an exception of *de facto* ownership (Ducuing, 2020).

201. The dominant conservative economics view of data is that it is a club good. Based on a way of classifying goods in neo-classical economics, this means that it is non-rival, i.e., its consumption by one individual would not prevent others from consuming it, as well as excludable, i.e., that its consumption could be prevented by organizational, technical or legal mechanisms (Purtova & Maanen, 2023).

202. The logic behind this classification is aimed ensuring that there is an adequate quantity and quality of data available in the market. Therefore, the focus shifts to data, itself as a resource and as an object of governance, to create incentives for their production and availability. However, if the purpose is to achieve other societal goals, even with the aid of data, like privacy, democracy, and sustainability, these goods are the ones that need to be conceptualized (Purtova & Maanen, 2023, pp. 21, 50).

203. An important problem with this approach, as described by Purtova and Maanen (2023), is its performative effect, as this view alters the very way humans interact with and value not only goods but also other people. The “market” becomes the standard against which these relationships and society as a whole are evaluated. This treatment of data as a commodity has

direct or indirect consequences, reinforcing harmful practices such as surveillance, creating problematic dependencies, and exploiting those involved in data production.

204. Moreover, adopting the neo-classical economic vocabulary may lead to market principles infiltrating non-market areas of life where exchange and commodification are not suitable, such as in family and community relationships (Purtova & Maanen, 2023, pp. 51–52). As the emphasis shifts towards collecting and producing increasingly more data, human life and social relations begin to be shaped to enable it. More broadly, understanding data as a commodity and the market as the standard for human relationships directly affects our individual and societal autonomy, ultimately calling into question our humanity and dignity.

3.5 Data colonialism and its incursion into autonomy

205. As explained above, this new data-mediated social configuration brings serious consequences for human autonomy. First, Couldry and Mejias (2019, p. 157) argue that autonomy is being harmed by the mere fact that data are being mandatorily collected as a requirement of daily life. Data colonialism not only potentially but in principle and by design affects the self's sphere of action because of its ubiquity. Every social relation is increasingly being datafied and embedded in data-driven technologies, which makes it very difficult for individuals to opt out, especially when it comes to essential services like education. And that is why one can speak of an increasingly extensive state of surveillance. Even if technologies are not being used for this immediate purpose (such as security cameras or behavior monitoring), individual and collective life is increasingly tracked in a disguised manner, thereby fostering a new layer of surveillance. This pervasive monitoring engenders a chilling effect, altering people's behavior as they are constantly observed.

206. Autonomy is also affected by the attempt to predict human behavior based on past behavior, which can restrict people's exposure to diverse perspectives, ideas, and opportunities, thereby limiting their possibility of exploring new and unanticipated paths. Data start to speak on people's behalf, which could also lead to violations of equity and non-discrimination.

207. Manipulation is also a very often outcome of commodification and DDBM, which implies that people's ability to make choices is compromised. Susser, Roessler and Nissembaum (2019, p. 4) argue that a critical aspect of manipulation is that it is a hidden practice. Manipulating someone would mean "intentionally and covertly influencing their decision-making by targeting and exploiting their decision-making vulnerabilities". This could

happen not only through deception but also by leveraging people's cognitive biases to influence the trajectory of decision-making (Susser; Roessler; Nissenbaum, 2019, p. 5). Through manipulation, autonomy is hampered in two main ways. First, it leads people to act towards ends they have not chosen. Second, their actions will be taken based on reasons that may not be their own.

208. People's digital profiles provide enough information for companies engaging in behavioral targeting to know precisely when to intervene to reach their goals most effectively. More than that, it enables the detection of specific vulnerabilities beyond the ones common to all human beings (such as related to unbounded rationality) (Susser; Roessler; Nissenbaum, 2019, p. 6)). Here, it is important to understand manipulation as a spectrum, as some practices can be more manipulative than others. In case of children, for example, the threshold for defining what is manipulative or not should be higher, as they are still developing their own discernment.

209. More generally, autonomy deeply impacts the educational experience, as it plays a pivotal role in fostering a dynamic and enriching learning environment, igniting students' intrinsic motivation and engagement. It fosters independence and self-confidence, empowering learners to take ownership of their educational goals and to take a broader part in society as a whole.

210. Given that autonomy is closely tied to safeguarding one's interests, it is logical to assume that eroding people's autonomy can lead to a reduction in pursuing them. As datafication continues to permeate every aspect of human life, there is a growing concern that we may progressively "unlearn" how to be autonomous (Couldry; Mejias, 2019, p. 173). In the case of children, they can grow up in a world where being autonomous is not even a possibility in the first place. Children are highly susceptible to manipulation (Giannini, 2023, p. 5) and these practices can affect the very development of children's autonomy and, consequently, how they value their own and other's privacy.

211. Finally, eroding autonomy also means eroding democracy and public institutions, as "it is only because we believe individuals can make meaningful independent decisions that we value institutions designed to register and reflect them" (Susser; Roessler; Nissenbaum, 2019, p. 11). Autonomy is at the core of liberal democratic societies, and it is only because individuals could potentially govern themselves that collective and democratic decisions can be made. The

incursion into democracy is deepened by the power asymmetry resulting from harvesting vast amounts of data and the fact that social knowledge is in the hands of only a few actors.

Interim conclusion

212. This chapter aimed to present the theory of data colonialism as a normative theory that will be used to evaluate the implications that current edtech have on children's rights to privacy and to the protection of personal data, as well as the extend to which the current legal framework deals with them. By appropriating human life and social relations and converting them into data, data colonialism can impact almost all of our actions and inner thoughts as they increasingly take place in the digital environment. This is not necessarily because we share them but because the infrastructure to collect observed and inferred data is becoming ever more ubiquitous and invasive, leading to an intricately, surveilled digital environment.

213. We have seen that historical colonialism and data colonialism share four key aspects: the appropriation of resources, unequal social and economic relations, unequal global distribution of the benefits of resource appropriation, and ideologies that help us make sense of the new order. Although discussed separately, these aspects are directly linked to one another. In order to appropriate data, the Cloud Empire needs to implement or make use of already existing unequal data relations. These relations are extremely asymmetrical due to (i) the opacity of the operations made with personal data, (ii) the overview of the social world that these companies have as a consequence, which is extremely powerful, and (iii) the fact that they are built on top of historical asymmetries, often as a product of historical colonialism. This exacerbates the global distribution of wealth and can only be justified by very specific narratives of datafication, connection, and techno-solutionism.

214. The Cloud Empire, implemented and extended by many players but primarily by the social quantification sector, directly benefits from the collusion or lack of states' action, which do not always act by the will of their people. This has caused the balance of knowledge to tip towards the side of a few technology companies, helped by a network of many other actors, generating a severe asymmetry of power that threatens our autonomy as individuals and as a collective.

215. The theory of data colonialism serves as a valuable framework for comprehending challenges associated with children's rights to privacy and to the protection of personal data in the digital realm, particularly with the use of edtech. Nevertheless, the solutions to these issues

are not readily apparent. Some ways to resist it will be briefly outlined in the conclusion of this thesis, encompassing the review of business models, the investment in sovereign and open source technology, the prohibition of data use for commercial purposes conflicting with educational objectives, the enforcement of protection by design standards, among others. However, promoting democratic and decolonial solutions presupposes that the process is as crucial as the content. Any attempt to oppose this order must be global in its *framing* (Couldry; Mejias, 2023, p. 793, 797), but the actual activities carried out must always consider the local specificities, including the community in imagining and designing them.

PART II. LEGAL FRAMEWORK ON CHILDREN'S PRIVACY AND DATA PROTECTION

216. Part II will describe and evaluate the current legal framework applicable to children's rights to privacy and to the protection of personal data in the EU and in Brazil. More specifically, I will focus on the rights enshrined in the CRC (Chapter 5), as well as on the GDPR (Chapter 6) and the LGPD (Chapter 7). Additionally, I will briefly present how AI is currently being specifically regulated in both jurisdictions, especially when it comes to data governance.

217. Before delving into these topics, however, I will discuss why children need special treatment by recognizing them as a subject of rights and adopting a children's rights perspective on privacy and data protection. This entails recognizing and prioritizing children's specificities while protecting and promoting these rights, as well as viewing their fundamental rights as indissociably connected to one another. Therefore, when one right is violated or realized, others are also affected. More specifically, the rights to privacy and to the protection of personal data are certainly an end in themselves but also importantly a means to realize other rights, such as the right to education. Only through this holistic view will we be able to properly allow children to grow autonomously and to their full potential as an individual and as a member of a larger collective.

Chapter 4. Why children need special privacy and data protection rights

218. The creation of a dedicated set of rights specifically tailored to children was not without its controversies, as some still argue that human rights codes already encompass all individuals, regardless of age. However, precisely because children are inherently less mature, more vulnerable, and in need of care and protection, their rights are frequently ignored, denied or abused, which demands a special treatment (Livingstone; O'Neill, 2014).

219. The CRC, as will be better discussed in Chapter 6, focuses on ensuring children are protected from harm, but also intends to foster the opportunities that can help children develop through provision and participation rights. Risks and opportunities, especially in the digital environment, are often linked—"the more one enables provision and participation, the more the need for protection; similarly, the more one seeks to protect, the more one risks undermining participation" (Livingstone; O'Neill, 2014, p. 28).

220. As a provision right, the right to education fosters children's development to their full potential and can be supported through edtech. As previously outlined in the introduction to this thesis, edtech offers numerous opportunities for learning, acquiring information, developing social, digital, and personal skills, as well as enhancing physical and mental abilities. This can prepare children for responsible life in a free society, as demanded by art. 29, CRC (Livingstone; O'Neill, 2014, p. 26). At the same time, the opportunities provided by edtech can create risks to children's rights, especially the rights to privacy and data protection, which is the direct focus of this thesis.

221. This chapter aims to highlight the unique characteristics of children that demand a special treatment in the digital environment. Section 4.1 will begin by discussing two main reasons why children deserve special treatment in this realm, namely their condition of human beings in development, which adds to them an extra layer of vulnerability, and their proportionally larger digital footprint when compared to adults. Section 4.2 will then outline a risk classification of children's online presence, which includes three main dimensions of privacy developed by Livingstone, Stoilova and Nandagiri (2018): interpersonal, institutional, and commercial. Finally, Section 4.3 underlines how surveillance technologies can significantly influence children's trust and development, impacting their ability to make independent decisions and fostering an environment that hinders their creativity and critical thinking.

222. Overall, the chapter underscores the need for a delicate balance between protection and autonomy, risks and opportunities, to ensure the holistic development of children in the digital era and, consequently, the exercise of their rights to education, privacy and data protection in their full potential.

4.1 Why do children's data require special treatment?

4.1.1 Childhood as an extra layer of vulnerability

223. Malgieri and Niklas (2020) conducted a thorough literature review on human vulnerability and propose a new vulnerability-aware interpretation of the rights to privacy and to data protection.

224. The authors show that discussions on vulnerability are traditionally focused on two dichotomies. One of them revolves around the particular and universal aspects of vulnerability. Vulnerability can be understood as a particular characteristic of a group or individual (such as children, people with disabilities, racial minorities, etc.). On the other hand, some theorists argue that this may lead to stigmatization and defend that vulnerability is a universal human condition—an approach criticized by some, as it tends to overlook structural issues experienced by specific groups or individuals (Malgieri; Niklas, 2020, p. 3).

225. Another important dichotomy is related to the consequences of being vulnerable. One of the approaches focuses on the harms and ways to eliminate them. Another is centered on the individual capacity to overcome this vulnerability through decisional and procedural safeguards in the decision-making process, such as consent (Malgieri; Niklas, 2020, p. 3–4).

226. Based on these dichotomies, the authors advocate that the best way to deal with vulnerability in general, and within privacy and data protection discussions in particular, is the layered approach developed by Luna (2009). She proposes that vulnerability should be understood dynamically and relationally (between the person or group and the circumstances) through layers (Luna, 2009). This notion obliges us to unravel the intricate layers and understand the intersectionality of different issues related to the context. A person's age, if they are a child for instance, can already be considered a layer of vulnerability. Additionally, we must also consider other aspects such as the specific age (due to the evolving capacities of the child), gender, race, country, nationality, health conditions, etc.

227. The extra layer of vulnerability children have is related to the fact that they are still developing physically, mentally, emotionally and spiritually. This means that they still depend, to a varying extent, on other people for protection, provision and decision-making (Sandberg, 2015, p. 222). Children's vulnerability can then be biological or socially constructed. Meyer (2007, p. 90) indicates that children can be

physically vulnerable (e.g. their bodies are smaller and weaker), socially vulnerable (e.g. they lack certain social skills) and structurally vulnerable (e.g. there are asymmetrical power relations between children and adults). Social and physical vulnerability are usually thought of as “innate” characteristics of the individual child and denote a lack of personal competence or strength. In contrast to this, structural vulnerability—as a lack of power—is a product of society.

228. The Committee on the Rights of the Child¹² also recognizes this horizontal vulnerability of children and specifies that

[a]t a universal level all children aged 0-18 years are considered vulnerable until the completion of their neural, psychological, social and physical growth and development. Babies and young children are at higher risk due to the immaturity of their developing brain and their complete dependency on adults [...] (Committee on the Rights of the Child, 2011, parag. 72(f)).

229. More specifically, the CRC states that some children deserve special attention, such as within the context of art. 23 on children with disabilities and art. 22 on asylum-seeking children. In its comments and jurisprudence, the Committee on the Rights of the Child also emphasizes the existence of subgroups of children with specific characteristics that require further protection (Sandberg, 2015). This aligns with Luna's layered approach mentioned above and also with the principle of non-discrimination enshrined in art. 2, CRC.

230. Children's vulnerability should not be interpreted in a paternalistic way, though, focusing on protection at all costs since it can stigmatize and hinder children's development. As a framework designed to address the specific vulnerabilities of children, the CRC (see *infra* Chapter 5) was established with a central emphasis on recognizing children as rights-holders, acknowledging their diverse capabilities and evolving capacities, and striving to strike a balance between various human rights in different circumstances. Recognizing children's vulnerabilities means, therefore, that they deserve a specific set of rights, including protection, provision and participation rights.

231. More specifically, in the data protection realm, data processing implications are already difficult for adults to understand, let alone for children. They are less experienced, especially

¹² The Committee on the Rights of the Child is the body of 18 independent experts that monitors the implementation of the CRC, as well as of its additional protocols. It also has a more “legislative” role, providing commentary on the interpretation of the Convention (United Nations Human Rights Treaty Bodies, [*s. d.*]).

in relation to possible risks and harms, and can be easily manipulated (Malgieri; Niklas, 2020, p. 5). For this reason, their agency is limited and others frequently take decisions related to their data on their behalf. There is also “a particular gravity to violations of children’s rights because they often have severe and long-lasting impact on child development” (Committee on the Rights of the Child, 2013b, parag. 24). Finally, they have fewer means for challenging the inferences and decisions made for them.

232. This links to the distinction between vulnerability risks related to data processing and the ones related to the outcomes of this processing (Malgieri; Niklas, 2020). Regarding the first one, risks can arise in terms of understanding information about data, what can hamper, for instance freely consenting when necessary, as well as effectively exercising data protection rights. From the second perspective, vulnerability is manifested through specific harms that children may be exposed to as a *result* of the processing of their data. Both of these sources of vulnerabilities will be developed further throughout the thesis.

4.1.2 A proportionally larger digital footprint

233. Apart from having an extra layer of vulnerability compared to adults, another aspect that demands a different approach in relation to children’s privacy and data protection is their “digital footprint” being proportionally larger than adults’. Children are being datafied before they are even born through, for example, parent’s searches on the internet, online purchases, ultrasound images publications on social media, and the use of pregnancy apps. Corporations have early access to important and sensitive data such as “conception date, weight, number of kicks in the womb, possible names, cultural background, heart rate, diet before conception, parents’ thoughts, family ties, family medical history, complications during pregnancy” among others (Barassi, 2020, p. 35).

234. After birth, the baby’s life continues to be tracked through growth-monitoring apps, wearables, smart toys, governmental apps and other data-driven technologies. Through smart assistants in the homes, as well as the children’s use of parents’ devices, children also have their data collected through technologies that are not necessarily appropriate to their needs. As mentioned earlier, the boundaries between individual and group data in data mining processes can be ambiguous. Therefore, children may also be profiled based on the behavior of their parents and the broader family.

235. This means that, unlike previous generations, children have all aspects of their lives turned into data points early on. Each year, a child will have more data collected about them throughout their life compared to a similar child born in previous years (Young; Verhulst, 2020). The older the child, the more they engage themselves in these practices, “but many other actors do so on their behalf, including not only their parents and other caregivers and family members, friends, teachers and healthcare providers but also commercial entities seeking to capitalize on and profit from children’s personal information” (Lupton; Williamson, 2017, p. 781).

236. Throughout history, children have, in fact, been subjected to surveillance as a means to enhance their well-being, foster their growth and educational development, and shape them into responsible members of society (Lupton; Williamson, 2017). With the rise of sharenting, parents have been constantly blamed for children’s digital presence. Indeed, this is a very problematic phenomenon of our current reality and cultural changes are needed to strike a proper balance between children’s rights and their parents’. However, it is essential to recognize that the vast majority of the data points collected from children do not necessarily originate from their parents’ practices. Companies’ interests play a significant role in encouraging and facilitating such data collection through technology’s design, the sale of wearables, connected toys, and other means.

237. Surveillance technologies are marketed primarily by highlighting the potential risks that children could face, taking advantage of parental worries and making intimate surveillance seem like an essential part of responsible caregiving. It is portrayed as a crucial aspect of being a parent and aligning with the social expectations and norms that new parents are expected to follow or adopt (Mascheroni, 2020, p. 805).

238. It is also important to highlight that tracking a family’s life is emotionally relevant to parents as it helps them to experience important moments, such as when family photos are taken. Family data tells a story that people like to share, and this has been done even before digital technologies (such as when parents journaled about a baby’s development, tracked their growth and took analogue photos) (Barassi, 2020). As this thesis will show, a closer look needs to be taken technologies’ data governance and business models in order to collectively solve a problem that cannot be tackled individually.

239. This is clearly shown by Vertesi (2014), who went through a self-experiment in which she tried to hide her pregnancy, which proved to be a challenging task. She had to refrain from

explicitly sharing it on social media (and also ensure that no one who knew her did) and from using pregnancy apps. She also had to use a private browser to look up baby names, as well as buy all pregnancy and baby-related items with cash. The attempt to “opt out” not only made her look rude to family and friends when they tried to bring up the topic online, but also like a criminal. She describes a situation where she had to purchase a large amount of gift cards with cash to buy a stroller online and the store displayed a notice indicating that it could limit the daily amount of prepaid card purchases and report excessive transactions to the authorities (Vertesi, 2014).

240. As a collective concern, the datafication of children’s lives poses significant challenges, primarily due to the uncertainties surrounding its future implications. While some of the effects on human rights, particularly in relation to children’s equitable access to education, employment, credit, and public services, are already discernible, the long-term cumulative effects of datafication remain unseen. Children’s vulnerability obliges us to think about the long-term impacts of technologies and the society we are building by datafying citizens from childhood.

4.2 Privacy and data protection as a cross-cutting dimension of risks to children’s online presence

241. Children are increasingly part of the digital environment, already accounting for one-third of all internet users (UNICEF, 2017). This participation holds significant importance in navigating today’s society and fostering children’s development. It provides them with opportunities such as staying in touch with friends and family, engaging in play, accessing information and education, and participating in democratic discussions. Children themselves, while consulted for the drafting of the Committee on the Rights of the Child’s General Comment No. 25, acknowledged that digital technologies are vital for their current lives and future (Committee on the Rights of the Child, 2021).

242. More than a way to enhance fundamental rights, digital technologies are increasingly the gateway for their realization, and children often have no choice whether they would like to use them or not for the most different purposes. Parents, educators, governments, and companies predominantly make these decisions on their behalf. In this sense, opportunities brought about by digital technologies need to be carefully balanced with the risks they pose to children’s rights, as they have reduced agency to exercise them and demand their realization.

The dynamic and ever-changing nature of the digital environment also means that risks are continuously evolving. As a consequence, children often find themselves encountering emerging risks long before adults are able to adequately tackle them (Siibak; Mascheroni, 2021).

243. It is also important to reinforce that fundamental rights are indivisible and interconnected. This means that the realization or infringement of one right automatically affects others. For instance, if steps are taken to protect children from potential online harm without concurrently considering their right to freedom of expression, the protective measures may excessively limit that freedom (Livingstone; Lievens; Carr, 2020). Therefore, in this session, a risk classification for children's online activities will be presented that takes into consideration different types and dimensions of risks.

244. Drawing from the online risk classification put forth by EU Kids Online in 2009 and an extensive literature review of similar initiatives, the CO:RE project introduces the 4Cs framework for understanding online risks children face. The 4Cs are content, contact, conduct and contract risks (Livingstone; Stoilova, 2021, p. 11):

Content risks: The child engages with or is exposed to potentially harmful content. This can be violent, gory content, hateful or extremist content, as well as pornographic or sexualised content that may be illegal or harmful, including by being age-inappropriate. Content online may be mass-produced or user-generated (including by the child), and it may be shared widely or not.


Contact risks: The child experiences or is targeted by contact in a potentially harmful adult-initiated interaction, and the adult may be known to the child or not. This can be related to harassment (including sexual), stalking, hateful behavior, sexual grooming, sextortion or the generation of sharing of child sexual abuse material.

Conduct risks: The child witnesses, participates in or is a victim of potentially harmful conduct such as bullying, hateful peer activity, trolling, sexual messages, pressures or harassment, or is exposed to potentially harmful user communities (e.g. self-harm or eating disorders). Typically conduct risks arise from interactions among peers, although not necessarily of equal status.

Contract risks: The child is party to and/or exploited by potentially harmful contractor commercial interests (gambling, exploitative or age-inappropriate marketing, etc.). This can be mediated by the automated (algorithmic) processing of data. This includes risks linked to ill-designed or insecure digital services that leave the child open to identity theft, fraud or scams. It also includes contracts made between other parties involving a child (trafficking, streaming child sexual abuse).

245. Each type of risk is divided into three dimensions in relation to its nature: aggressive, sexual and values. Additionally, apart from the 4Cs, the classification recognizes that some of the mapped risks are related to most or all the four categories, so they were considered cross-cutting risks (these include online risks related to privacy, physical or mental health, inequalities or discrimination), as depicted in the table below:

Figure 2 - The CO:RE classification of online risks to children

	Content Child engages with or is exposed to potentially harmful content	Contact Child experiences or is targeted by potentially harmful <i>adult</i> contact	Conduct Child witnesses, participates in or is a victim of potentially harmful <i>peer</i> conduct	Contract Child is party to or exploited by potentially harmful contract
Aggressive	Violent, gory, graphic, racist, hateful or extremist information and communication	Harassment, stalking, hateful behaviour, unwanted or excessive surveillance	Bullying, hateful or hostile communication or peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, hacking, blackmail, security risks
Sexual	Pornography (harmful or illegal), sexualization of culture, oppressive body image norms	Sexual harassment, sexual grooming, sextortion, the generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messaging, adverse sexual pressures	Trafficking for purposes of sexual exploitation, streaming (paid-for) child sexual abuse
Values	Mis/disinformation, age-inappropriate marketing or user-generated content	Ideological persuasion or manipulation, radicalisation and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, adverse peer pressures	Gambling, filter bubbles, micro-targeting, dark patterns shaping persuasion or purchase
Cross-cutting	Privacy violations (interpersonal, institutional, commercial) Physical and mental health risks (e.g., sedentary lifestyle, excessive screen use, isolation, anxiety) Inequalities and discrimination (in/exclusion, exploiting vulnerability, algorithmic bias/predictive analytics)			

Source: Livingstone & Stoilova (2021, p. 12)

246. The risks related to privacy are considered cross-cutting risks and they can be described in three main dimensions: interpersonal, institutional, and commercial. This framework was initially developed by Livingstone, Stoilova and Nandagiri (2018) based on Nissenbaum's theory of privacy as contextual integrity. It is important to mention that Nissenbaum's theory frames privacy in a broad way, including informational privacy, which would also be aligned with the right to the protection of personal data, as understood in the EU and Brazilian legal frameworks. The authors propose this division focusing on the importance of relationships and contexts in which children act for determining privacy risks, as well as on how children understand the implications for their privacy.

247. Interpersonal privacy is undoubtedly the aspect that children and their parents most focus their attention on, and it refers to the relationships between an individual and other individuals or groups. The decisions taken in the digital environment related to this domain are heavily influenced by how children perceive each context, what is the audience they interact with, and how they balance privacy with other wishes such as participation, self-expression and belonging (Livingstone; Stoilova; Nandagiri, 2018, p. 13)

248. Institutional privacy is related to public or third-sector (not-for-profit) organizations and how they handle children's data. Through exchanges with research participants, as well as a

literature review, Livingstone, Stoilova and Nandagiri (2018, p. 13) identified that the collection of data by these entities is often perceived as legitimate, and people do not express concern about the purpose of data collection or the potential long-term consequences of data processing. However, the involvement of governments and other entities in creating children's digital footprints, their ability to request data from private entities, and the sharing of data with other governmental entities can pose significant risks to children's rights. As previously mentioned, it is also crucial to note the increasingly intertwined relationships between public and private entities, particularly facilitated by digital technology. This convergence not only blurs traditional boundaries but also enhances the level of integration, consequently intensifying associated risks (Livingstone; Stoilova; Nandagiri, 2018, p. 14).

249. Finally, commercial privacy pertains to the processing of children's data by commercial entities. As the private sector is currently gathering more data than governments ever did (Nyst; Gorostiaga; Geary, 2018), there is a preoccupation with how they process children's data and the tactics they use to access larger amounts of them. Despite this area's importance, the authors identified a gap in the available empirical evidence related to children's awareness of commercial data gathering and its consequences. Although existing research shows the existence of certain commercial privacy concerns, children typically exhibit a degree of confusion regarding the concept of personal data and generally struggle to grasp why their data could hold value for others (Livingstone; Stoilova; Nandagiri, 2018, p. 14–15).

250. Within these three contexts, children experience privacy risks that, apart from being a problem in itself, can affect other dimensions, as presented in Figure 1. Hence privacy being considered a cross-cutting risk. The list is extensive and encompasses online marketing and other problematic commercial activities, reputational damage, blackmailing, stalking, identity theft, unwanted contact with strangers, location tracking, manipulation, discrimination and biased decisions, and the potential limitation of future opportunities (Livingstone; Stoilova; Nandagiri, 2018, p. 28–30).

251. Within the school environment, edtech poses significant risks to children's privacy and data protection, as they often process a large amount of data, especially for AI-powered edtech. These data can be aggregated to create detailed profiles of students that can be used for purposes not necessarily aligned with their best interests. Education data can inform decisions across a wide range of areas and serve as input for commercial and governmental strategies. The lack of proper data protection measures can thus directly impact several fundamental rights, such as the right to education, freedom to choose an occupation and non-discrimination more broadly.

The specific challenges edtech brings to children's privacy and data protection will be discussed in Part III.

4.3 The importance of privacy and data protection for children's development and learning

252. A critical dimension to consider when evaluating the impacts of edtech on children is its influence on their opportunities to trust and to be trusted. As previously noted, the ubiquity of digital ICTs, coupled with a prevalent business model that encourages the commodification of data and its massive collection, plunges us into a constant state of surveillance. Therefore, the following discussion directly pertains to technologies specifically designed for monitoring children in educational settings, such as behavior tracking or e-proctoring systems. However, it also extends to seemingly innocuous or low-risk technologies that form part of a broader network of stakeholders and data sharing practices, potentially compromising children's rights in a similar fashion.

253. The use of surveillance technologies to monitor and control children can promote an approach to childhood that aims to leave little to chance and achieve a risk-free environment. This approach ignores the importance of balancing trust and risk and the opportunities for children to negotiate terms of freedom and develop skills and competencies (Rooney, 2010).

254. By creating unease and fear, surveillance technologies have the potential to change a child's experience of trust and even replace trust-based relationships. Children perceive surveillance as a means of control that restricts their options and hampers their capacity to act independently. Getting information through surveillance assumes that children cannot be trusted. It can influence their behavior by using punishment and reward as motivating factors instead of moral principles. This type of guidance deprives children of the chance to try out critical and ethical decision-making, ultimately leading to reduced self-regulation and autonomy (Nolan; Raynes-Goldie; McBride, 2011).

255. When children are monitored without their knowledge, it can be even more harmful to their trust in the adult. The deception involved in secret monitoring can damage the very foundation of trust. Therefore, using surveillance technologies can actually increase suspicion instead of fostering a sense of security (Rooney, 2010).

Children, generally speaking, have less choice when it comes to the need to trust others, and are at a key stage in developing an understanding of others and society more broadly in a way that sets the foundation for their own sense of self. [...] [T]he lack of opportunity for trust-based activity has the potential to undermine a child's

developing sense of self-confidence and may even fail to provide the conditions for this development to occur in the first place. A child's capacity to become competent and responsible is therefore threatened if the role of trust in a child's emerging agency is overlooked rather than nourished" (Rooney, 2010, p. 353).

256. Children need to develop their own knowledge and skills to judge about potentially harmful information or people online. Trusting a child can help them develop skills and competencies for dealing with difficult situations, whereas the opposite may lead to more secretive and risky behavior. This is not to say that balancing trust and risk is not a complex issue for all actors involved in a child's development, who must consider whether they are protected from harm and whether certain technologies can help achieve this. However, avoiding risks altogether is unrealistic and when selecting the technologies children will interact with (if they are to be used at all), other factors should also be factored in (Rooney, 2010).

257. Surveillance technologies also affect the development of autonomous children and the way they understand privacy. The development of individual autonomy is crucial for both social and socio-emotional development during early childhood. By exploring autonomous actions, children learn to understand their role in society within a specific socio-cultural context, which helps them become capable adults (Nolan; Raynes-Goldie; McBride, 2011, p. 25). Developing autonomy is also tied to fostering various aspects of their growth, including identity formation, independence, responsibility, individuation, resilience, and self-expression. Additionally, it is crucial for properly developing prosocial behavior, forming strong and trusting relationships, and enhancing critical thinking skills (Nolan; Raynes-Goldie; McBride, 2011, p. 25–26).

258. In contrast, heteronomous children tend to view choices in terms of rewards or punishments rather than critically evaluating them. For instance, heteronomous children typically believe that lying is wrong only if they get caught and punished, but it is acceptable if they do not. Heteronomy can be present in various aspects of a child's life, not only in relation to their parents but also through education, religion, and other institutional structures that reinforce reward and punishment (Nolan; Raynes-Goldie; McBride, 2011, p. 26), such as in the use of surveillance technologies in education.

259. In the context of healthy socio-emotional development, privacy and autonomy are intertwined and dependent on each other (Nolan; Raynes-Goldie; McBride, 2011, p. 27). Autonomy is essential for individuals to exercise their privacy and data protection rights, allowing them to make decisions free from external influence. Conversely, privacy and data protection are also crucial for children, as they need their own space to reflect on their values, beliefs, and preferences without manipulation or other external interference. This is especially

important during the development of these values, as surveillance technologies may interfere and impact a child's perception of them.

260. If children cannot experience privacy in their daily lives, they may not develop the ability to establish and advocate for their own boundaries and privacy, or even recognize the boundaries of others. This heteronomous conditioning may be a contributing factor to the prevailing perception of today's youth as being inappropriate "over-sharers" who do not appreciate or value privacy (Nolan; Raynes-Goldie; McBride, 2011, p. 27).

261. In early childhood, children exhibit a desire for privacy and autonomy by engaging in acts of independence and resistance to authority, such as making a mess or noise or running away when called. However, this raises the question of whether it is possible to cultivate genuine autonomy in spaces where children are under constant surveillance and their only means of resisting heteronomy is through secrecy or subversion (Nolan; Raynes-Goldie; McBride, 2011, p. 27).

262. This also hampers creativity and experimentation, preventing individuals from expressing themselves freely due to the fear of consequences. Ultimately, it can stagnate society since these experimentations cannot slowly become commonplace, moral, and/or legal. "All social progress—from ending slavery to fighting for women's rights—began as ideas that were, quite literally, dangerous to assert" (Schneier, 2018).

263. This directly affects the possibility of implementing a quality education that focuses on the holistic development of human beings. If children cannot trust the space and the adults who take care of them while being educated, this causes them to reduce their participation due to fear of making mistakes and being reprimanded. Considering that making mistakes is inherent and essential to get things right within the school environment, we might witness a generation struggling not only with learning but also with becoming critical and creative citizens who can navigate the world's problems.

Interim conclusion

264. In this chapter, the aim was to present the reasons why children need special protection in relation to the rights to privacy and to the protection of personal data. I first described the theory of layers of vulnerability as developed by Luna (2009) and why being a child is an extra layer that entails special attention. This was complemented by the fact that children were born

in a world where the analogue and the digital are in tandem like never before, meaning that their digital footprint is proportionally larger than previous generations’.

265. I also discussed why privacy and data protection are a cross-cutting dimension of risks to children’s online presence, which will be complemented in Part III by the specific risks brought about by edtech. Finally, I have presented why privacy and data protection are important for the development of children as a whole, especially for their autonomy, which is extremely important for education.

266. The multifaceted nature of children’s presence in the digital environment demands a comprehensive and nuanced approach that acknowledges their unique characteristics and developmental needs. Edtech has the potential to offer unprecedented opportunities for learning, accessing information, and developing physical, social, and digital skills. As presented in the introduction to this thesis, these benefits should be acknowledged as an important opportunity to take education to the next level, promoting more access and equity for all children. Recognizing that opportunities are often associated with risks, however, the former should be balanced with the need to cater to other rights, striving for a delicate balance between protecting children and allowing them to develop autonomously as human beings.

Chapter 5. The CRC in the digital environment

267. The CRC was unanimously adopted on November 20, 1989 by the UN's General Assembly. It is so far the most ratified human rights treaty in history, with currently 196 parties (Nations Unies, 2023). Especially during a time of changing world order, the CRC brought about a significant paradigm shift. Children should not be viewed as mere possessions of their parents or miniature adults. Instead, children began to be internationally recognized as rights holders (UNICEF, [s. d.]).

268. The CRC fully applies to the digital environment, as the latter has become an integral part of children's lives, both positively and negatively impacting several of the rights enshrined therein. These rights are affected even when the child does not have access to the internet or other technologies themselves (Committee on the Rights of the Child, 2021). More evidently, the lack of access to digital ICTs itself compromises rights such as education, information, and social interaction. However, more indirectly, children are also affected by the spread of misinformation; by decisions made about them based on their data, even without their participation; and by the regulation (or lack thereof) of the digital environment.

269. To implement the rights-based approach described in the introduction to Part II, the following subsections will describe how some provisions outlined in the CRC are interconnected with the use of data-driven edtech, and, more specifically, affect children's right to privacy and to the protection of personal data.

270. Considering that the CRC is a comprehensive framework, I will focus on the provisions that are considered cross-cutting standards (being used to guide the interpretation or implementation of other rights) or that directly links to the scope of the thesis. As defined by Hanson and Lundy (2017), the concept of cross-cutting standards largely overlaps with the idea of general principles, as described by the Committee on the Rights of the Child. It is then important to briefly explain the idea of the CRC's general principles, how they came to be, as well as why this thesis does not fully adopt this concept.

271. Originally, the CRC did not make any hierarchical distinction in relation to its provisions nor mention the idea that some of them should be used to interpret and implement the rest of the Convention. The term "general principles" was introduced by the Committee on the Rights of the Child in its general guidelines on periodic reporting in 1996 (Doek, 2007). The Committee identified these principles as arts. 2, 3, 6 and 12 of the CRC, i.e., the right to

non-discrimination; the right to have the child's best interests taken as a primary consideration; the right to life and development; and the right to have their views given due weight in accordance with their age and maturity.

272. The idea of the general principles is largely adopted by scholars and have been widely used by many stakeholders. However, it was not included within the CRC itself and its meaning was not thoroughly developed by the Committee (Hanson; Lundy, 2017). It remains unclear, for example, why these specific provisions were selected as general principles and not others (Lundy; Byrne, 2017). Indeed, some provisions have an intersecting role in relation to all articles of the Convention, as evident from their wording and practical interpretation, such as arts. 2, 3, and 12, as will be detailed below. However, art. 6 on the right to live, survival and development "sits uncomfortably as a provision with a cross-cutting role" (Hanson; Lundy, 2017, p. 301).

273. It is evident that the right to life is a child's most fundamental human right since its fulfilment is a precondition for the realization of all other fundamental rights. In the same way, realizing all other rights enshrined in the CRC contributes to the child's survival or development. Nevertheless, it is not easy to grasp the added value of this right for the interpretation or implementation of other articles in the CRC (Doek, 2007, p. 37).

274. Having this in mind, Hanson and Lundy (2017) propose an alternative conceptualization. They argue that it is possible to identify in the CRC some "overall implementation obligations" related to implementing legislation, setting up of national bodies, development of policies, etc., such as arts 4, 41, 42, and 44 parag. 6, CRC. They also identify some substantive cross-cutting standards¹³ that, as mentioned above, will be important to interpret and implement the CRC as a whole. The authors propose replacing art. 6 by art. 5 on the child's evolving capacities as it has been recognized not only by different child rights actors but also by the Committee (see *infra* Section 5.3) as having a cross-cutting role. The subsections below will then adopt this alternative conceptualization and also discuss the rights to privacy,

¹³ The authors "choose the word 'cross-cutting' rather than 'general', or 'overall' because it directly expresses what these provisions do: they cross-cut or intersect with and apply to all other articles. We propose the word 'standard' since the common usage of this term expresses, in a general descriptive manner, a substantial norm and also refers to a required level of quality that can be measured. The term 'standard' hence expresses the two main functions of the four provisions (non-discrimination, best interests of the child, respect for the evolving capacities and respect for the views of the child) which are to provide a framework to interpret the CRC as well as to assess progress made with the implementation of the Convention as a whole" (Hanson; Lundy, 2017, p. 302).

education, and protection against economic exploitation as enshrined in the CRC, since they are directly related to the core focus of the thesis.

5.1 The right to non-discrimination

275. Neither art. 2, CRC, nor the Committee on the Rights of the Child define the concept of “discrimination”. However, the latter has already invoked some elements of the right to non-discrimination that can help understand it. This right can be defined as “the prohibition of treating similar situations differently without an objective justification” (Besson; Kleber, 2019).

276. Besson and Kleber (2019, p. 60–64) identify and analyze three elements from this definition. First, discrimination implies an unfavorable treatment of any kind, be it a different treatment in similar situations or similar treatment in different situations. There is no need to show intent to discriminate, which means that it encompasses both direct and indirect discrimination.

277. The second element is the necessity of this discrimination to be based on a prohibited ground. Art. 2(1), CRC, provides a list of discriminatory grounds, but this list is purely indicative and can be extended to other similar grounds. It is also important to mention that art 2(2), CRC, extends this protection to discrimination or punishment based on the child’s parents, legal guardians, or family members’ characteristics. Linked to the discussion on the existence of layers of vulnerability is the emphasis by the Committee that discrimination can be based on multiple grounds (multiple discrimination). In a concrete case, it may be challenging to separate these grounds, but they are “useful to highlight the especially vulnerable position of children in society, and the Convention’s lack of explicit protection against discrimination based on age together with other grounds” (Besson; Kleber, 2019, p. 63).

278. Finally, a third element is the absence of justification. The Committee on the Rights of the Child (2016, parag. 21) is of the opinion that “not every differentiation of treatment will constitute discrimination, if the criteria for such differentiation are reasonable and objective and if the aim is to achieve a purpose that is legitimate under the Convention”. Ultimately, the mere existence of the CRC and of a framework that specifically recognizes children’s rights already target a justifiable differentiation between children and adults. Here, the principle of the best interests of the child can be understood as a tool to help justify differential treatments, either between children and adults or between children themselves (Besson; Kleber, 2019, p. 64).

279. In the digital environment, discrimination manifests in multiple ways, such as in unequal access to technology or hate speech. More important for this thesis, though, is the potential for discrimination stemming from biased algorithms. As exemplified before, this can happen “when automated processes that result in information filtering, profiling or decision-making are based on biased, partial or unfairly obtained data concerning a child” (Committee on the Rights of the Child, 2021, parag. 10). This also occurs when children in different regions of the world have varying levels of protection concerning their personal data, not necessarily due to the absence of minimal legal protection regarding the technologies that affect them, but rather due to the lack of enforcement and the presence of economic incentives conflicting with their fundamental rights.

5.2 The right to have the child’s best interests taken as a primary consideration

280. Art. 3, 1, CRC, provides children with the right to have their best interests taken as a primary consideration in all actions that concern them. This is not a new concept and was first introduced in the 1959 Declaration on the Rights of the Child. Here, it is important to understand the meaning of best interests and what is the role of this right in the CRC.

281. The best interests of the child is purposefully an indeterminate concept, and it will vary according to different societies and historical periods. An interesting definition is given by John Eekellar, who understands it as “[b]asic interests, for example to physical, emotional and intellectual care; developmental interests, to enter adulthood as far as possible without disadvantage; autonomy interests, especially the freedom to choose a lifestyle of their own” (Eekellar, 1992, 230-231, as cited in Freeman, 2007, p. 27).

282. Determining what is in the best interest of a child or group of children must necessarily be done through a rights-based approach, considering all the rights enshrined in the CRC. Ultimately, this is an open and dynamic concept and will largely depend on the assessment of the specific context where it is applied (Committee on the Rights of the Child, 2013a).

283. In its General Comment on the matter, the Committee on the Rights of the Child does not attempt to prescribe what is in the best interests of a child in any given situation but provides a framework for identifying it. It recognizes three primary roles of this right. First, it is a substantive right, which means that children need to have their best interests taken as a primary consideration (the child’s interests have high priority and should not be seen as just one of several considerations) when different interests are being considered and whenever a decision

concerning the child is taken. Second, when it is possible to interpret a legal provision in multiple ways, the interpretation that best serves the child's best interests should be selected, having as a basis the rights recognized by the CRC (best interests understood as a fundamental, interpretative legal principle). Finally, it is also a rule of procedure, and an evaluation of the positive or negative impacts of a decision on the child or group of children should be included in every decision-making process that could affect them (Committee on the Rights of the Child, 2013a, parag. 6).

284. It is important to mention that this applies not only to decisions made within the scope of the state, but also to the ones made by the private sector, "including those providing services, or any other private entity or institution making decisions that concern or impact on a child" (Committee on the Rights of the Child, 2013a, p. para 14, (c))

285. In a concrete case, in order to define what the best interests actually are, the Committee provides the following parameters:

- a) The universal, indivisible, interdependent and interrelated nature of children's rights;
- b) Recognition of children as right holders;
- c) The global nature and reach of the Convention;
- d) The obligation of States parties to respect, protect and fulfill all the rights in the Convention;
- e) Short-, medium- and long-term effects of actions related to the development of the child over time (Committee on the Rights of the Child, 2013a, parag. 16).

286. For this thesis, the last criterion is especially important. In the decision-making process, decision-makers will mainly focus on the current interests of the child, which are often formulated in relation to experiential considerations (Freeman, 2007, p. 3). Nevertheless, future interests that are frequently more focused on developmental considerations (Freeman, 2007, p. 3) should also be taken into account. The right to have the child's best interest into consideration should also be seen as a *precautionary principle*, which "requires assessing the possibility of future risk and harm and other consequences of the decision for the child's safety" (Committee on the Rights of the Child, 2013a, p. 74). The understanding obliges us to act cautiously even when the potential danger of a certain technology is not fully established, but there are indications that not acting upon them could inflict harm. This is especially true for the decisions related to the use of technologies, the benefits of which are not confirmed by scientific evidence (Lievens, 2021). We can thus say that the precautionary principle flips the coin and adds extra importance to proving that technology does good rather than proving that it actually causes or will at some point in the future cause harm.

287. Here, the link with the evolving capacities of the child should also be made. The maturity of the child should not only be considered when assessing their best interests but also be used as a criterion for reassessing the decision over time. The scenarios of the child's development should be taken into account, and "decisions should assess continuity and stability of the child's present and future situation" (Committee on the Rights of the Child, 2013a, parag. 84).

288. As a General Measure of Implementation for the CRC, the best way to identify and balance all the interests involved in a decision that affects children is to perform a Child-rights Impact Assessment (CRIA) (Committee on the Rights of the Child, 2003). Every policy, whether intended or not, has a positive or negative impact on the lives of children (Payne, 2019) and understanding the role of art. 3, 1, as a rule of procedure demands states to explain, in every decision, what has been considered in the child's best interest, which criteria have been used, and how different interests have been weighed (Committee on the Rights of the Child, 2013a, parag. 6).

289. Although initially targeting state's initiatives, this tool was later also extended to businesses (Mukherjee; Pothong; Livingstone, 2021), especially under the UN Guiding Principles on Business and Human Rights (United Nations Human Rights. Office of the High Commissioner, 2011).

Child-rights impact assessments can be used to consider the impact on all children affected by the activities of a particular business or sector but can also include assessment of the differential impact of measures on certain categories of children. The assessment of the impact itself may be based upon input from children, civil society and experts, as well as from relevant government departments, academic research and experiences documented in the country or elsewhere. The analysis should result in recommendations for amendments, alternatives and improvements and be publicly available (Committee on the Rights of the Child, 2013b, parag. 80).

290. The Committee's understanding has been reinforced in its General Comment 25, which focuses on the impact of the digital environment on children's rights. CRIAs should be carried out by businesses "with special consideration given to the differentiated and, at times, severe impacts of the digital environment on children" (Committee on the Rights of the Child, 2021, parag. 38).

States parties should require all businesses that affect children's rights in relation to the digital environment to implement regulatory frameworks, industry codes and terms of services that adhere to the highest standards of ethics, privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of their products and services. That includes businesses that target children, have children as end users or otherwise affect children. They should require such businesses to maintain high standards of transparency and accountability and encourage them to take measures to innovate in the best interests of the child.

They should also require the provision of age-appropriate explanations to children, or to parents and caregivers for very young children, of their terms of service (Committee on the Rights of the Child, 2021, parag. 39).

291. Given its rapid pace of change and complex nature, especially in relation to its long-term consequences, the digital landscape particularly requires the use of such tools. Many stakeholders agree that “if CRIA were used effectively, and its results evaluated transparently, it will make a real difference to realizing children’s rights in a digital world” (Mukherjee; Pothong; Livingstone, 2021, p. 26).

5.3 The right to be given appropriate direction and guidance in a manner consistent with the evolving capacities of the child

292. The reference to “evolving capacities” happens twice in the CRC in art. 5 and art. 14(2). Both are related to parental direction and guidance and do not create by itself a right of the child to exercise the rights enshrined in the convention based on their evolving capacities. They actually recognize the right of children to receive parents’ and guardians’ due guidance and to secure the realization of these rights according to their evolving capacities (Tobin & Varadan, 2019, as cited in Varadan, 2019, p. 308). More broadly, it can be understood as a principle that addresses the processes of children’s maturation, as well as their acquisition of competencies, understanding, and agency to assume more responsibility and exercise their rights. This should directly impact their parents’ guidance towards an exchange on an equal footing (Committee on the Right of the Child, 2016, parag. 18; Committee on the Rights of the Child, 2009, parag. 84).

293. However this concept has taken a broader role over time. Having analyzed all the comments and jurisprudence from the Committee on the Rights of the Child that mention the notion of evolving capacities, Varadan (2019) concludes that the Committee has indeed recognized it as a principle that should be used while interpreting and implementing the CRC, confirming the need to include it as a cross-cutting standard, as defended by Hanson and Lundy (2017). The Committee’s understanding can be categorized into three distinct groups:

1) “evolving capacities” as an enabling principle, in which the term is used to empower children in the exercise of their rights under the UNCRC; (2) “evolving capacities” as an interpretative principle, in which the term is used to interpret specific provisions of the Convention in a manner that recognizes children’s capacities in the exercise of their rights; (3) “evolving capacities” as a policy principle, in which the term is used to guide states in policy-making and programming on children’s rights (Varadan, 2019, p. 316).

294. Understanding the evolving capacities of the child as a principle has profound implications for children's human rights. Is crucial for striking a balance between "recognising [them] as active agents in their own lives, entitled to be listened to, respected and granted increasing autonomy in the exercise of rights [... and] being entitled to protection in accordance with their relative immaturity and youth" (Lansdown, 2005, p. 3).

295. These three categories can be directly applied when children navigate the digital environment and specifically when they are supposed to use edtech. When it comes to empowering children by recognizing children's evolving capacities, data protection frameworks can include means for them to actively and autonomously participate in decisions regarding their personal data. Examples would include enabling children to consent to the processing of their personal data or exercise certain data subject rights depending on their complexity. The Committee emphasizes that the right to exercise increasing levels of responsibility does not mean that other protective measures should not apply (Committee on the Right of the Child, 2016, parag. 19).

296. Viewing the evolving capacities as an interpretative principle implies that data protection laws should be interpreted and applied in a way sensitive to children's developmental stages and respect their evolving understanding of privacy and data protection. Finally, as a policy principle, it could translate into discussions of age appropriateness, which refers to "a developmental concept whereby certain activities may be deemed appropriate or inappropriate to a child's 'stage' or level of development" (Cassidy, 2013, p. 83). This is because the risks and opportunities faced by the child in this realm will vary according to their age and stage of development (Committee on the Rights of the Child, 2021, parag. 19). Many DPAs in Europe, in this sense, have already issued specific guidelines interpreting the data protection laws according to children's specificities, helping controllers to act in accordance to children's evolving capacities and assisting technologists in designing with this principle in mind.

5.4 The right to have their views given due weight in accordance with their age and maturity

297. Art. 12, CRC, guarantees the right for children to express their views freely and be given due weight in all matters that affect them, according to their age and maturity. It is closely linked to the concept of participation, which are ongoing processes that "include information-sharing and dialogue between children and adults based on mutual respect, and in which children can learn how their views and those of adults are taken into account and shape the

outcome of such processes” (Committee on the Rights of the Child, 2009, parag. 3). The idea of participation also emphasizes that this should be not only a momentary act, but the foundation for an ongoing dialogue between children and adults in the development of policies, programs, and measures across all areas of children’s lives (Committee on the Rights of the Child, 2009, parag. 13).

298. In order to better understand the scope of this right, it is important to unpack some of its foundational aspects. First, children should have the ability to freely express their views. The term “freely” implies that no pressure should be exerted upon the child, allowing them to decide whether or not to exercise this right. Additionally, it entails that children should not be manipulated or subjected to undue influence or pressure and that they should be able to express their own perspectives rather than adopting the opinions of others (Committee on the Rights of the Child, 2009, parag. 22).

299. Children also need to have their rights to freedom of expression (art. 13, CRC) and access to information (art. 17, CRC) fulfilled. The latter is indeed a prerequisite to the right to be heard, as children need information to take well-informed stances and make decisions. This includes “matters, options and possible decisions to be taken and their consequences [... as well as information] about the conditions under which she or he will be asked to express her or his views” (Committee on the Rights of the Child, 2009, parag. 25). The Committee also emphasizes that children should receive all the information and advice to make a decision in favor of their best interests (Committee on the Rights of the Child, 2009, parag. 16). The quality of the information received by the child should be child-friendly, comprehensible according to their age and maturity, and accessible.

300. Simply hearing the child is not sufficient. Their views should be seriously considered in accordance with their age and maturity. Considering that children’s level of understanding are not homogeneously linked to biological age, the Committee included the criterion of maturity, which refers to “the ability to understand and assess the implications of a particular matter” (Committee on the Rights of the Child, 2009, parag. 30).

301. In its General Comment on the matter, the Committee also explicitly provides guidance on hearing children’s views in the school environment, as it is fundamental to the realization of the right to education and to address issues such as bullying and discrimination. It emphasizes the importance of encouraging children’s active engagement within a participatory learning

setting, particularly when it comes to designing curricula and school programs (Committee on the Rights of the Child, 2009, parag. 107). States parties should also

consult children at the local and national levels on all aspects of education policy, including, inter alia, the strengthening of the child-friendly character of the educational system, informal and non-formal facilities of learning, which give children a “second chance”, school curricula, teaching methods, school structures, standards, budgeting and child-protection systems (Committee on the Rights of the Child, 2009, parag. 111).

302. In the digital realm, the right to be heard could be promoted through consultative online processes, for example. States parties should also involve all children in the development of legislation, policies, programs, services and training on children’s rights targeting this environment. It is also their role to ensure that “digital service providers actively engage with children, applying appropriate safeguards, and give their views due consideration when developing products and services” (Committee on the Rights of the Child, 2021, parag. 17–18). Realizing this right in the context of datafication is especially important when the dominant discourse is that data can speak for themselves.

303. The right to be heard and, consequently, the right to participate hold particular significance in selecting and implementing technologies within schools. Involving children in decision-making processes regarding the edtech used in their educational environments empowers them to shape their learning experiences, including how their rights to privacy and data protection are considered; ensures that edtech meets the diverse needs and preferences of the student body; and fosters a sense of ownership and accountability, ultimately leading to more effective and inclusive educational practices.

5.5 The right to privacy

304. Art. 16, CRC, basically mirrors art. 12 of the Universal Declaration of Human Rights (UDHR) and art. 17 of the International Covenant on Civil and Political Rights. However, this provision should be interpreted through a child-centric approach, given the different ways that children experience privacy in comparison to adults (Schmahl, 2021). It aims to protect six different but related interests against arbitrary or unlawful interference: privacy, family, home, correspondence, honor, and reputation. The literature often includes all these interests within the concept of privacy, which is justified by a broad understanding of it (Tobin; Field, 2019).

305. Although the concept of privacy is widely used, it has never been properly defined, neither by the Committee on the Rights of the Child, nor by the Human Rights Committee.

However, having analyzed the jurisprudence of international human rights bodies, Tobin and Field (2019) identified the development of at least five dimensions of this right: physical and psychological integrity; decisional autonomy; personal identity; informational privacy; and physical/spatial privacy. For the purposes of this thesis, I will focus on the second, third and fourth dimensions.

306. The decisional autonomy dimension is related to “the capacity to make decisions regarding how an individual leads his or her private life” (Tobin; Field, 2019, p. 565). This idea poses a challenge for children due to child’s maturity and a potential conflict between a child and their parents. Both issues can be solved by a contextual analysis of the child’s best interests and evolving capacities. This is also a relational concept and includes the autonomy of a child to enter into relationships with others.

307. Privacy is also related to the ability to freely express one’s identity. The concept of a child’s identity would include, for instance, “the rights to a name, a nationality, to be registered immediately after birth, as well as elements of a child’s religious and cultural identity” (Tobin; Field, 2019, p. 568). This right to identity is key to accessing other rights, as it is related to the very recognition of children as rightsholders.

308. Finally, the informational privacy dimension is closely linked to the control of personal information and, therefore, to the right to the protection of personal data. The analyzed jurisprudence reinforces that it applies the access to data created by a person for personal use (such as in personal diaries or text messages) as well as, more broadly, information about a child that either public or private actors can hold.

309. The protection of personal data is an essential safeguard since many children’s activities now take place in the digital environment. Practices such as “automated data processing, profiling, behavioral targeting, mandatory identity verification, information filtering and mass surveillance are becoming routine [... and] may lead to arbitrary or unlawful interference with children’s right to privacy” (Committee on the Rights of the Child, 2021, parag. 68).

310. In its General Comment n. 25, the Committee on the Rights of the Child states that surveillance and automated processing of data should not only respect children’s rights to privacy but also not be

conducted routinely, indiscriminately or without the child’s knowledge or, in the case of very young children, that of their parent or caregiver; *nor should it take place without the right to object to such surveillance*, in commercial settings and educational and care settings, and consideration should always be given to the least

privacy-intrusive means available to fulfil the desired purpose (Committee on the Rights of the Child, 2021, p. 75, emphasis added)

[...] By introducing or using data protection, privacy-by-design and safety-by-design approaches and other regulatory measures, States parties should ensure that businesses do not target children using those or other techniques designed to prioritize commercial interests over those of the child (Committee on the Rights of the Child, 2021, parag. 110).

311. This is especially important when considering the use of technology in education, as it highlights the inherent power imbalances among educational institutions, technology providers, and students/their parents. Unfortunately, in many instances, individuals are left with no viable option to opt out of pervasive surveillance and select a less intrusive technological solution.

312. More specifically, the Committee emphasizes that processing children's data may lead to the violation of their rights, such as "through advertising design features that anticipate and guide a child's actions towards more extreme content, automated notifications that can interrupt sleep or the use of a child's personal information or location to target potentially harmful commercially driven content" (Committee on the Rights of the Child, 2021, parag. 40). It also explicitly states that

States parties should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling. Practices that rely on neuromarketing, emotional analytics, immersive advertising and advertising in virtual and augmented reality environments to promote products, applications and services should also be prohibited from engagement directly or indirectly with children (Committee on the Rights of the Child, 2021, parag. 42).

313. Considering all these dimensions of the right to privacy, according to international human rights bodies' jurisprudence, it is important, however, to avoid a purely protectionist approach. While shielding children from potential risks that may be encountered in the digital environment is a legitimate aim, this should be balanced against the realization of other rights, such as freedom of expression, freedom of association and even education (Lievens *et al.*, 2019). The right to privacy, understood broadly, is essential but is just one of the human rights of children that should be considered in decision-making processes in any given case.

5.6 The right to education

314. The right to education is widely accepted and recognized and, in its enabling role, is essential for enjoying many other human rights. It is a prerequisite for engaging in political activities and ensuring the proper operation of democratic systems; a requirement for many

employment opportunities; a valuable resource to deal with poverty; and a factor that deeply influences individuals' well-being and environmental health (Courtis; Tobin, 2019, p. 1058).

315. The right to education is thus vital to empower children, “providing them with the skills necessary to be on guard against exploitation in all its forms, understand democracy and human rights” (Courtis; Tobin, 2019, p. 1060), as well as enjoy a “well-educated, enlightened and active mind, able to wander freely and widely” (Committee on Economic Social and Cultural Rights, 1999a, parag. 1).

316. Although generally classified as an economic, social and cultural right, its centrality for the enjoyment of civil and political rights defies human rights classifications and “epitomizes the indivisibility and interdependence of all human rights” (Committee on Economic Social and Cultural Rights, 1999b, parag. 2). It should be then recognized both as a right with an intrinsic value and as a multiplier right (Tomaševski, 2001, p. 10), “whose aims promote, support and protect the core value of the Convention: the human dignity innate in every child and his or her equal and inalienable rights” (Committee on the Rights of the Child, 2001, parag. 1).

317. The CRC addresses the right to education in two provisions. Art. 28 recognizes the existence of a right to education in and of itself and mainly focuses on the issues of access to education. Art. 29 addresses the aims of education, directing the actions of State parties in relation to the quality of the education that should be provided. The CRC adopts a holistic notion of education that includes not only the acquisition of knowledge, but also “the development of life skills necessary to realize a child’s full potential within the broader context of the community and environment in which the child lives” (Courtis; Tobin, 2019, p. 1063).

318. This holistic understanding of the role of education in individuals and society is fully aligned with the educational concept adopted in this thesis, based on Freire, as discussed in Chapter 1. By viewing history as a possibility, children as individuals whose agency should be fostered, and education as the engine of change towards a more egalitarian world, we realize how reductionist it is to treat education merely as synonymous with “learning”. Considering the current landscape of available edtech, this broad view of education has yet to be solidified and embedded in technologies.

319. Katarina Tomaševski, the first UN Special Rapporteur on the Right to Education, suggests the “4As” conceptual framework to identify qualitative dimensions of education that should be implemented in order to fully realize the right enshrined in art. 28, CRC. According

to this framework, states have the obligation to make education available, accessible, acceptable and adaptable (Tomaševski, 2001).

320. The dimension of availability is related to states' obligation to make enough resources available to fulfil children's educational rights, as well as to allow the establishment of educational institutions by non-state actors (Tomaševski, 2001). Accessibility refers to the need for education to be open to all. This implies non-discrimination, physical accessibility, and economic accessibility. Acceptability means that

the content of education and teaching methods is relevant, culturally appropriate, and of good quality. [...] The meaning of quality is to be determined by reference to the extent to which a state is able to provide an educational setting which is consistent with the broad and general aims of education outlined in article 29 of the Convention (Courtis; Tobin, 2019, p. 1069).

321. Finally, adaptability relates to the need for education to be flexible to the student's needs and contexts (e.g. students with disabilities, working children, children in situations of humanitarian crises etc.) (Tomaševski, 2001), as well as to the challenges that an evolving society poses (Courtis; Tobin, 2019).

322. These dimensions that should inform the realization of the right to education, as stated in art. 28, CRC, are closely related and establish the link to art. 29, CRC, which describes the aims of education. The very first General Comment issued by the Committee on the Rights of the Child was focused on art. 29, CRC, and it understands that education should provide children with life skills. This includes not only literacy and numeracy but also the capacity "to make well-balanced decisions; to resolve conflicts in a non-violent manner; and to develop a healthy lifestyle, good relationships and responsibility, critical thinking, creative talents, and other abilities which give children the tools needed to pursue their options in life" (Committee on the Rights of the Child, 2001, parag. 9). Education should then "embrace the broad range of life experiences and learning processes which enable children, individually and collectively, to develop their personalities, talents and abilities and to live a full and satisfying life within society" (Committee on the Rights of the Child, 2001, parag. 2).

323. The Committee also emphasizes that education should be child-friendly and developed in an environment that allows children to grow based on their evolving capacities. This means that the kind of teaching, as well as methods and technologies used within education, that focus "primarily on accumulation of knowledge, prompting competition and leading to an excessive burden of work on children, may seriously hamper the harmonious development of the child to

the fullest potential of his or her abilities and talents” (Committee on the Rights of the Child, 2001, parag. 12).

324. Art. 29 challenges an instrumentalist view of education, which considers education a tool for children to ensure economic prosperity and social cohesion (Lundy; Tobin, 2019, p. 1117). Although these are valid and welcomed objectives, the key goal of education should be the “[...] development of the individual child’s personality, talents and abilities, in recognition of the fact that every child has unique characteristics, interests, abilities, and learning needs” (Committee on the Rights of the Child, 2001, parag. 9). More broadly, “the enjoyment of the right to education is not conditioned upon, or subordinated to, the achievement of instrumental societal goals” (Curtis; Tobin, 2019, p. 1062–1063). The list included in art. 29 also rejects “strict individualism in favor of a relational conception of rights in which children are aware of the rights and interests of others and their moral obligation to assume a constructive role in their society” (Lundy; Tobin, 2019, p. 1122).

325. The digital environment has the potential to enhance the right to education and its aims recognized in art. 28 and 29, CRC. It can increase access to education and support learning opportunities in extracurricular activities. It can also qualitatively improve education, as children can access more information and educational resources and exchange their views with more people. However, as described above, providing education through digital technologies poses many challenges. Among the specific recommendations specified by the Committee on the Rights of the Child for fulfilling the right to education in the digital environment, two should be highlighted.

326. First, procurement and use of educational technologies by state parties should adhere to evidence-based policies, standards, and guidelines. These technologies must be ethically sound, suitable for educational purposes, and ensure the protection of children from violence, discrimination, data protection violations, and commercial exploitation, among other potential risks (Committee on the Rights of the Child, 2021, parag. 103).

327. Second, digital literacy is of vital import so children gain an understanding of the digital environment’s “infrastructure, business practices, persuasive strategies and the uses of automated processing and personal data and surveillance, and of the possible negative effects of digitalization on societies” (Committee on the Rights of the Child, 2021, parag. 105). Media literacy should serve a dual purpose for children and young individuals, encompassing both a protective and a participatory aspect. It equips them with the necessary skills and competencies

to navigate and control their online presence. Policies and initiatives concerning media literacy should thus be developed in alignment with all children's human rights (Lievens *et al.*, 2019, p. 500) and the school curriculum appears to be the best place to discuss and implement these initiatives with children and educators.

5.7 The right to protection against economic exploitation

328. Art. 32, 1, CRC, recognizes the child's right to be protected from economic exploitation. Although the interpretation of this provision is generally focused on the protection against child labor, it is possible to understand this right in a much broader sense. Verdoodt (2020) proposes to separate this right in two to argue for the expansion of its interpretation. First, "economic" indicates a material interest, namely, the pursuit of gain or profit through the production, distribution, or consumption of goods and services. This material interest can influence the economy at various levels, such as the state, the community, or the family. Second, "exploitation" refers to unfairly taking advantage of others for one's own advantage or benefit. Specifically, this encompasses actions like manipulation, misuse, abuse, victimization, oppression, or ill-treatment (Verdoodt, 2020, p. 98).

329. The broader understanding of these elements allows us to recognize them in the digital environment, as already described above. The need to prioritize children's best interests over commercial interests in the digital environment has also been recently emphasized by the Committee on the Rights of the Child. In its General Comment 25 (2021), the Committee highlighted how commercial interests can negatively impact children's rights to independent information (parag. 53), children's freedom of expression (parag. 61), and children's right to play (parag. 110).

330. More specifically on the negative impacts on children's data protection, the Committee is of the opinion that a) profiling and targeting must not occur for commercial purposes¹⁴; b) surveillance should not be part of a child's routine and they have the right to object to it in

¹⁴ "States parties should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling. Practices that rely on neuromarketing, emotional analytics, immersive advertising and advertising in virtual and augmented reality environments to promote products, applications and services should also be prohibited from engagement directly or indirectly with children." (Committee on the Rights of the Child, 2021, parag. 42).

commercial, educational and care settings¹⁵; and c) privacy- and safety-by-design approaches should be implemented to prioritize children's rights over commercial interests¹⁶.

331. We should note that although the CRC is not legally binding to the private sector, based on the UN Guiding Principles on Business and Human Rights,

the Committee recognizes that duties and responsibilities to respect the rights of children extend in practice beyond the State and State-controlled services and institutions and apply to private actors and business enterprises. Therefore, all businesses must meet their responsibilities regarding children's rights and States must ensure they do so [...] (Committee on the Rights of the Child, 2013b, parag. 8).

332. It would be fair to argue that students and their parents would not expect that their data be used for purposes unrelated to their education (Chakroun *et al.*, 2022). The Consultative Committee of Convention 108, for instance, stated that “educational institutions need strong legislative frameworks and codes of practice to empower staff, and to give clarity to companies to know what is permitted and what is not when processing children's data in the context of educational activities, creating a fair environment for everyone” (CoE, 2021, p. 7). The Global Privacy Assembly is also of the opinion that “States should consider promoting regulations prohibiting the use or transmission to third parties of children's data for commercial or advertising purposes and the practice of marketing techniques that may encourage children to provide personal data” (Global Privacy Assembly (GPA), 2021, p. 6).

333. The discussion on the legitimacy of a for-profit approach to student's data and its impact on children's rights is intrinsically related to the business models of edtech solutions as discussed in Chapter 3. It prompts us to consider how the commodification of data may provide the incentive to collect and process increasingly larger amounts of children's data in ways that prioritize profit over their well-being and rights. Therefore, discussing the effectiveness of the current data protection gal framework becomes necessary, considering that they still do not focus on the root of many of these problems.

¹⁵ “Any digital surveillance of children, together with any associated automated processing of personal data, should respect the child's right to privacy and should not be conducted routinely, indiscriminately or without the child's knowledge or, in the case of very young children, that of their parent or caregiver; nor should it take place without the right to object to such surveillance, in commercial settings and educational and care settings, and consideration should always be given to the least privacy-intrusive means available to fulfil the desired purpose” (Committee on the Rights of the Child, 2021, parag. 75).

¹⁶ “Leisure time spent in the digital environment may expose children to risks of harm, for example, through opaque or misleading advertising or highly persuasive or gambling-like design features. By introducing or using data protection, privacy-by-design and safety-by-design approaches and other regulatory measures, States parties should ensure that businesses do not target children using those or other techniques designed to prioritize commercial interests over those of the child” (Committee on the Rights of the Child, 2021, parag. 110).

Interim conclusion

334. The CRC is a pivotal milestone in the history of children's rights, representing a paradigm shift in societal perceptions and treatment of children. Their unique needs stemming from their evolving capacities and inexperience give rise not only to protective rights but also to provision and participation rights, fostering their holistic development.

335. This chapter aimed to highlight CRC provisions most pertinent to the scope of this thesis. I presented a reconceptualization of the CRC's core principles developed by Hanson and Lundy (2017), outlining four provisions crucial for implementing and interpreting all other rights in the Convention. These include the rights to non-discrimination, to have their best interests taken as a primary consideration, to be given appropriate guidance aligned with their evolving capacities, and to have their views given due weight according to their age and maturity. I elaborated on how these cross-cutting standards influence the interpretation of children's data protection, offering some examples of their application in edtech.

336. Additionally, I discussed other significant provisions, notably the right to privacy (broadly interpreted), the right to education, and the right to protection against economic exploitation. In the realm of education, technologies should be part of a comprehensive strategy aligned with the educational objectives mandated by art. 29, CRC, rather than being adopted solely for convenience or because they are freely available. Such technologies must also harmonize with children's rights to privacy and protection against economic exploitation. This entails that if other interests, such as commercial ones, clash with the right to privacy, or if there is a foreseeable risk of harm from the technology in the future, the child's best interests should serve as both an interpretative guide and a precautionary measure.

Chapter 6. EU's relevant legal and policy frameworks

337. The right to privacy as a human right was recognized in art. 8 of the European Convention on Human Rights (ECHR) in 1950 and has been broadly interpreted to encompass the protection of personal data (European Court of Human Rights, 2022). This is crucial for interpreting the rights enshrined in the Charter of Fundamental Rights of the European Union (CFR), as the interpretation of the latter must be informed by the interpretation of the ECHR by the European Court of Human Rights (ECtHR). Moreover, when applying the CFR, it is essential to ensure that the level of protection provided is, at a minimum, equivalent to that offered by the ECHR, according to art. 52(3), CFR.

338. In the 1960s, many European countries started to realize the potential risks to privacy and human autonomy that arose with technological developments. This has led to various waves of laws that intended to regulate the processing of personal data, as well as to the recognition of data protection as a fundamental right in national constitutions. The German federal State of Hesse was the first to adopt a legal act on governmental records in 1971, and Sweden was the first European country to introduce a national-wide regulation in 1973 (Vogiatzoglou; Valcke, 2022, p. 13).

339. In 1980, the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were adopted by the OECD, representing the world's first international statement of principles governing data processing. The principles focused on the protection of privacy and individual liberties and the guidelines were intended to balance it with the free flow of information (González Fuster, 2014).

340. The Council of Europe (CoE)'s Convention 108 was also adopted in 1980 and opened for signature in January 1981. It was mainly driven by an understanding that although the national data protection regimes shared fundamental principles, there were significant disparities that justified further action (González Fuster, 2014, p. 86). Unlike the OECD Guidelines, it formally aimed to ensure data protection. However, it was also directly concerned with securing the free flow of data, and its preamble links it to the freedom of information across frontiers. This was mainly influenced by the exchange that occurred between the Committee of Experts on Data Protection and the OECD since the first meeting to discuss the Convention. They had a common view that the Convention should "respect the principle of free international flow of information as supported by the OECD, and to refrain from laying

obstacles in the way of international trade and commerce” (Hondius, 1978, p. 8, as cited in González Fuster, 2014, p. 87).

341. On the EU level, the first legislation on the topic was the Data Protection Directive (DPD (European Union, 1995)), which was adopted in 1995 and remained in force until the GDPR application in 2018. Heavily influenced by the DPD and the increasing use of personal data to fuel new technologies, the CFR, adopted in 2000 (but becoming binding only in 2009) recognized not only the right to respect for privacy and family life, in its art. 7, but also the protection of personal data in its art. 8 as a separate right (Fabbrini, 2015). The entry into force of the Lisbon Treaty in 2009 also led to important developments for the data protection right in the EU (Kranenborg, 2021). It was explicitly recognized both in art. 16 of the Treaty on the Functioning of the European Union (TFEU), and art. 39 of the Treaty on the European Union (TEU). Furthermore, the CFR was granted legal binding force.

342. The separation of the two rights in the CFR was, however, not obvious, and there is still intense scholarly discussion concerning their relationship, particularly the nature and role of the right to data protection (Vogiatzoglou; Valcke, 2022). The case law of the Court of Justice of the European Union (CJEU) often presents these two rights in an interwoven manner (González Fuster; Hijmans, 2019, p. 4) and, when discussing art. 8, “generally uses a secondary law parlance” (Vogiatzoglou; Valcke, 2022, p. 22). Therefore, the risk of downgrading the fundamental right to data protection to the level of secondary law should be considered. This could potentially limit its content and protective value, opposing the prevalence of EU primary law over EU secondary law (Vogiatzoglou; Valcke, 2022, p. 22).

343. Although the discussion about the adequacy and differentiation of these two rights is not the focus of this thesis, it is essential to highlight their relevance to the conceptualization of data protection in Europe. Ultimately, the separate consideration of personal data protection from privacy, aiming to promote the free flow of information, may serve as the foundation for the current regulation of data as itself a subject of law. Therefore, it is crucial to understand the challenges and potentials of art. 8 as a standalone right (Vogiatzoglou; Valcke, 2022), especially when this interpretation could provide a higher level of protection for citizens’ fundamental rights.

344. Apart from arts. 7 and 8, CRF, it is also important to briefly highlight the importance of art. 24, CRF, on the rights of the child, as it could also influence the way we interpret children’s rights to privacy and to the protection of personal data. According to its explanation note, art.

24 is “based on the New York Convention on the Rights of the Child signed on 20 November 1989 and ratified by all the Member States, particularly Articles 3, 9, 12 and 13 thereof” (European Union, 2007b). The provision does not adopt the exact wording of the CRC provisions but rather reformulates them in a less detailed way (Lamont, 2021, parag. 24.45). Contrary to what one might expect, the provisions it is based on are not exactly the CRC so-called general principles or overarching standards, but an interesting mix of the right of the child to have their best interests considered as a primary consideration; the right of the child not to be separated from their parents against their will; the right to be heard; and the right to freedom of expression.

345. The TFEU defines no direct competence over the general promotion of children’s rights. However, different aspects of EU Law directly impact children, which means that art. 24 has the potential to shape the development and interpretation of EU measures concerning children (Lamont, 2021, parag. 24.03). The inclusion of this right in the Charter was also seen as a symbolic shift towards recognizing children as rights holders (Lamont, 2021, parag. 24.48).

6.1 The General Data Protection Regulation (GDPR)

346. This section will serve the purpose of a functional analysis of the GDPR, aiming to map key provisions related to the challenges identified in Part III of this thesis. I will specifically focus on provisions targeted at the specificities of children, as well as the ones regarding principles, transparency obligations, roles and responsibilities, legal bases, data subject rights, and the necessity of performing risk/data protection impact assessments.

6.1.1 General Principles

347. Art. 5, GDPR, outlines general principles to be followed when processing personal data. Throughout the various generations of data protection laws in Europe, these principles have undergone few modifications (Terwangne, 2020a), demonstrating the growing importance and stability of data protection fundamentals. They serve not only as the starting point for more detailed provisions throughout the regulation (European Union Agency for Fundamental Rights (FRA), 2018), but also as a means to interpret it. The principles are lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.

348. The GDPR highlights the specificities of the processing of children's data in the principle of lawfulness (art. 6(1)(f) and art. 8, GDPR), and transparency (art. 12(1), GDPR). Although considered a cornerstone of data processing, the principle of fairness is not further elaborated in the GDPR. Fair processing of personal data is closely related to the analysis of the reasonable expectations of the data subject, but what it means exactly, especially in the case of children, is still unclear (Milkaite, 2021, p. 206). The rights enshrined in the CRC, especially the principles of the best interest of the child, evolving capacities, the right to be heard and the right to non-discrimination, should be used as a means of defining what are children's reasonable expectations and how they can be incorporated into the processing of their personal data.

349. It is also important to highlight the principles of purpose limitation and data minimization, as they should be more strictly interpreted when it comes to processing children's data (Article 29 Data Protection Working Party (WP29), 2013a, p. 26). The principle of purpose limitation encompasses two sub-principles: purpose specification and compatible use. This means that, first, the purpose of the data processing must be specified prior to the data collection and they should be legitimate, explicit and unambiguous understood by all parties. Second, data cannot be further processed for purposes not aligned with the original one (Drechsler; Vogiatzoglou, 2023). Aligned with this principle is data minimization, which mandates that only data necessary to fulfil a certain purpose be processed.

350. In the era of big data and complex AI systems, however, when the mindset of understanding data as an economic good prevails, these two principles face significant challenges in their application. As we will further discuss in Part III, advanced AI systems, especially ML ones, depend on large amounts of data to be trained and to perform their activities. The way they function also makes it difficult to determine which exact piece of data influenced the inferences or decisions, complicating even further the assessment of data minimization. Especially regarding general-purpose AI, developers may not always foresee all their potential applications, leading to possible changes in the purposes for which data will be processed along the way.

351. Given the challenges already posed by applying these principles to data processing by ML algorithms, we should understand how they can be interpreted even more strictly for processing children's data. In this regard, comprehending the rationale behind these principles in the GDPR can help guide the interpretive approach.

352. The principle of purpose limitation in the GDPR exists for various reasons, such as narrowing down the scope of the processing operation, serving as a factor of foreseeability of data processing activities, and as a barrier to concentration of informational powers. It also enhances legal certainty, transparency, accountability, and individual's trust. At the same time, the possibilities for further use offer a balanced approach between individuals' interests and the pragmatic needs from other public or private actors (Drechsler; Vogiatzoglou, 2023; Ducuing; Schroers, 2020).

353. In order to interpret the purpose limitation and data minimization more strictly, we should shift the focus to the interests of other involved parties beyond the data subject, particularly regarding further use of data. Given that the best interests of children should *primarily* be taken into consideration, other interests should only prevail when they overwhelmingly outweigh children's rights.

354. When conducting the compatibility test outlined in art. 6(4), GDPR, one must assess how the fact that the data are from children influence the assessment. Examples include considering the nature of the data; strengthening the link between the purposes for which data have been collected and the purposes for which they are going to be further processed; the potentially heightened consequences for child data subjects; and the expectations of children as data subjects, which, as mentioned above, can be particularly challenging to grasp as they are still developing their discernment and should be interpreted according to the realization of their rights within the CRC.

355. These general principles can be better implemented through the principle of data protection by design and by default using appropriate technical and organizational measures (art. 25, GDPR) to put in practice a comprehensive and holistic approach to children's rights (Hof; Lievens, 2018, p. 2). According to recital 78, GDPR, these measures include

minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features.

356. The list above is non-exhaustive and controllers must be creative while implementing other measures and safeguards that are appropriate to the nature, scope, context and purposes of the data processing. Based on the accountability principle, "[a]n organization should be able to show how the best interests principle has driven the design, development, implementation and/ or operation of any service which is directed at/ intended for, or is likely to be accessed

by, children and how measures implemented are effective in achieving this” (Data protection Commission (DPC), 2021, p. 63).

6.1.2 Roles and responsibilities

357. The roles and responsibilities described in the GDPR do not change when children’s data are processed. Nonetheless, interpreting the requirements of the GDPR appropriately, as well as understanding the challenges posed by complex AI supply chains and by certain specific situations within edtech, will be crucial for the analysis conducted in Part III.

358. The concepts of controller and processor as described in the GDPR are functional concepts, which means that roles should be identified solely based on an assessment of the factual elements or circumstances of the case (European Data Protection Board (EDPB), 2021, parag. 12). According to art. 4(7), GDPR, the data controller is

the natural or legal person, public authority, agency or other body which, alone or jointly with others, *determines the purposes and means of the processing of personal data*; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law (emphasis added).

359. To be able to determine the purposes and means of the data processing (the “why” and “how”, the actor should be able to truly exercise the decision-making power, which could stem from legal provisions or the factual influence (EDPB, 2021, parag. 21). The level of influence of each actor will certainly vary depending on the situation, which requires that clear criteria be defined in order to draw the line, especially when processors are involved.

360. The EDPB is of the opinion that decisions on the purpose of the processing are always for the controller to make, while decisions in relation to the means can be done by both controllers and processors. What needs to be considered in relation to the latter is if the means are essential or not:

“Essential means” are means that are closely linked to the purpose and the scope of the processing, such as the type of personal data which are processed (“which data shall be processed?”), the duration of the processing (“for how long shall they be processed?”), the categories of recipients (“who shall have access to them?”) and the categories of data subjects (“whose personal data are being processed?”). Together with the purpose of processing, the essential means are also closely linked to the question of whether the processing is lawful, necessary and proportionate. “Non-essential means” concern more practical aspects of implementation, such as the choice for a particular type of hard- or software or the detailed security measures which may be left to the processor to decide on (EDPB, 2021, parag. 40).

361. When the public school is providing the edtech to children, the school will likely be the controller for the majority of the processing activities, meaning that most of the compliance

obligations will fall on them. The edtech provider, as a processor, will be basically the “digital extension of the school’s offline activities and the school exercises the decisive influence over the processing. [The] edtech product or service is not merely helpful for the school, but forms an integral part of the school’s functions” (Information Commissioner's Office (ICO), 2023a, n.p.).

362. From the case law of the CJEU, we can ascertain that the concept of controller should be understood broadly, in order to protect data subjects and encompass those who exert influence over the processing of personal data for their own purposes, participating, as a result, in the determination of the purposes and means of that processing (European Union, 2018a). To exert influence includes, for instance, defining parameters, contributing to determining the purposes of another controller’s processing, and making processing by other controllers possible (European Union, 2018b, 2019).

363. An example can elucidate how this functions in practice. When schools procure a LMS to provide a digital platform for teachers to upload assignments, they enable the processing of students’ and staff members’ data by the LMS provider. The schools also establish the purpose of the processing, which in this case is to realize the functionality provided by the LMS provider.

364. This remains the case even when the school does not have access to the data directly (EDPB, 2021). For instance, if the platform employs algorithms for personalized learning, the means of the processing (algorithmic analysis) and the purposes (enhancing individualized learning experiences) are determined by the school which procured the service for this specific finality.

365. Defining the roles, however, is not always so straightforward. First, because the platform can participate in defining the essential means of the processing activities such as which data is processed; for how long they are processed; if decisions are automated etc. Second, platforms may exert influence or engage in processing for their own purposes that are not directly related to providing the contracted service. If the platform process personal data for their own purposes beyond what is necessary to deliver the requested service to the customer or influence the purposes of processing operations for their own commercial gain (so more or different types of data are collected in the first place, for instance), they cannot be considered a processor anymore (Cobbe; Singh, 2021).

366. When the edtech provider wants to be a controller for its own purposes, another relationship with the data subject will need to be established, such as through a separate contract. On the other hand, according to the EDPB guidelines on the matter, joint controllership may be identified when decisions about the data processing are inextricably linked (EDPB, 2021). Therefore, if the edtech provider intends to process data for its own purposes that it accessed solely due to the contract with the school, then the school will necessarily be considered a joint controller. In this case, the school could only participate in such a joint controllership if the data processing activity is part of its mandate.

6.1.3 Article 8, GDPR

367. Unlike the DPD, the GDPR (European Union, 2016) contains specific provisions focusing on protecting children's data. Recital 38, GDPR, sets the tone of this special protection, stating that

[c]hildren merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.

368. Based on the need for a special protection, art. 8 outlines the specific conditions under which consent can be used as a lawful basis for processing children's data by Information Society Services (ISS). As a general rule, consent should be given or authorized by the holder of parental responsibility until the child reaches 16 years of age. However, MS could lower it until 13 years. This section will aim to explain the specificities of this provision.

6.1.3.1 ISS

369. The rule contained in art. 8 solely applies to ISS. These services are defined in art. 4(25), GDPR, through a cross-reference to the art. 1(1)(b) of the Single Market Transparency Directive. They should be understood as

any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: (i) 'at a distance' means that the service is provided without the parties being simultaneously present; (ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request.

370. This is a comprehensive definition and will encompass almost any online service. For the purposes of this thesis and for the applicability of art. 8 to the use of edtech within the school environment, it is important to clarify two aspects.

371. First, regarding the necessity for remuneration, it should be understood broadly (Kosta, 2020). According to the CJEU caselaw, remuneration does not need to come directly from the user through a monetary transaction in so far as the service represents an economic activity (European Union, 2014, parag. 28–29). There is also no need for the provider of the service to be seeking to make a profit, which would encompass the provision of the service for educational, charitable or recreational purposes as well (European Union, 2007a, parag. 34; Tosoni, 2020, p. 297). Additionally, it is possible to argue that in the cases where the service is provided on a non-profit basis, but it is still commonly provided on a for-profit basis, then it will be considered to be “normally provided for remuneration” (ICO, 2023b).

372. Second, it is important to clarify what an individual request is. As mentioned above, under the Single Market Transparency Directive, this means that the service is provided through the transmission of data upon individual request. This would not include, for example, television and radio broadcasting services as clarified by Annex I of the Directive. Within the CJEU caselaw, the *Mediakabel* case is an interesting example of how this requirement is interpreted. *Mediakabel* was a pay-per-view service where users would order a film from their catalogue using their personal identification. The CJEU did not consider it to be a service at the individual request since the list of films available for watching is solely determined by the service provider (European Union, 2005, parag. 38–39; Tosoni, 2020).

373. This raises the question of whether edtech services provided for or procured by schools would fall under this definition. One could argue that even if the school is an intermediary in relation to the provision of the service, if the student or their parents need to create an account or log in to use the service, or even interact individually with a service using a school device, this could already be considered as an individual request for data to be transmitted (Hooper; Livingstone; Pothong, 2022, p. 12).

374. However, in cases where the school assumes the role of controller in processing activities, it seems evident that they do not fall within the scope of art. 8, as they would not be considered ISSs. As we will delve into further below, using consent as a legal basis within the school environment will often prove unsuitable due to the inherent power imbalance between them and the data subjects. Nonetheless, in situations where consent is deemed appropriate and

art. 8 does not apply, the question arises regarding the possibility of using this legal basis at all, as well as the appropriate age for providing consent and who should provide it if not the child. If we consider that consent is still a possible legal basis, it appears that the age of majority rules governing civil acts in each country will need to be applied instead of art. 8, GDPR.

6.1.3.2 Offering directly to a child

375. The application of art. 8, GDPR, also depends on the service being provided directly to a child. In order to better protect children's best interests, we should interpret this provision broadly. The provision should not be understood to cover only services exclusively built for children (such as YouTube Kids, Messenger Kids, or other services solely focused on children). If children are also a target audience for the service, along with adults, parental consent should also be obtained depending on the child's age (Kosta, 2020). If a service intends to exclude children from its usage, it is crucial to clarify that they only offer their services to adults (EDPB, 2020, parag. 130).

376. Based on the fairness, accountability and data protection by design principles, it is possible to argue that all necessary measures should be taken to effectively prevent children from using it and merely stating this in their ToS would not be enough. This is also supported by the EDPB when it argues that more important than what is stated by the service is the evidence related to the actual offering of the service to children (EDPB, 2020, parag. 130).

377. If the service is not directed to a child and still needs to process children data for any reason, art. 8 would not apply, and national laws on age majority will need to be complied with. Still, data should be processed in children's best interest, and all principles of the GDPR should be interpreted based on that.

6.1.3.3 Age for consent

378. Art. 8 is a clear attempt to balance the fact that children are rights holders with evolving capacities and their need for special protection. Determining an age at which certain rights should be acquired or certain protections should be lost is a complex issue (UNICEF, 2007, p. 1). As the UN Special Rapporteur on the right to privacy puts it,

[c]hildren's readiness for decision-making and self-responsibility is best determined not by chronological age alone but by context, including the risks and support available, individual experience, the rights affected and capacity for understanding the implications of their actions (or non-actions). Determinations on when children are capable, for example, of consenting to the processing of their personal data, must take into consideration their actual understanding of the data processing, their best interests, rights and views (Cannataci, 2021, parag. 114).

379. As previously discussed, this should ideally be done on a case-by-case basis as each child grows and develops their capacities at varying ages. However, especially while formulating policy and legislation, these decisions should consider children as a group.

380. When this is the case, recognizing the best interests of the child as a rule of procedure will necessarily require an evaluation of the decision's impacts on the specific group of children being targeted. Children should be involved in the process to ensure their right to be heard is fulfilled. However, it appears that this was not the case when determining the age range for consent to be included in the GDPR (Carr, 2016; Lievens, 2016).

381. The impact assessment that accompanied the GDPR states that the rules for consent that require parental authorization took direct inspiration from the USA's Children's Online Privacy Protection Rule (COPPA) of 1998. According to the document, this would benefit online businesses since they would not "impose undue and unrealistic burden upon providers of online services and other controllers" (European Commission, 2012, p. 68).

382. Instead of assessing the provision's impact on children's rights, as mandated by the CRC, the Commission relied on a foreign rule implemented to benefit businesses. The threshold for consent in COPPA itself was also not based on empirical evidence but was the product of political compromise (Macenaite; Kosta, 2017, p. 183). The rule that emerged for online marketing in the 1990s can also poorly reflect the need for greater protection in today's digital environment, where children's data are processed in an unprecedented volume.

383. Research carried out by Livingstone and Ólafsson (2017), based on data from UK, indicates that children's commercial literacy tends to increase consistently from the age of 8 to young adulthood. Additionally, there would be a noticeable enhancement in commercial literacy between the ages of 13 and 16. It is uncertain whether these outcomes apply to the entirety of Europe. As previously mentioned, various factors in children's development influence their vulnerability and the acquisition of specific skills at different times and in different ways. Nonetheless, these findings highlight how such evidence can be readily collected to inform policymaking and enhance the protection of children's fundamental rights.

384. Within the EU, MS have selected all possible ages to establish the consent threshold, which would hinder the goal of achieving consistency under the GDPR. The implementation of art. 8 has resulted in a fragmented scenario, making it challenging for data controllers to conduct their operations within the EU (Milkaite, 2021, p. 168–169). This is also problematic because

it creates a form of discrimination among children from different countries without clear justifications (Milkaite, 2021, p. 170).

6.1.3.4 Consent as an appropriate legal basis for processing children's data

385. In societies that foster individual freedom, consent plays an important role as a legal and ethical tool for status change. Consent legitimizes an act that would otherwise be initially illegal or immoral (Kim, 2019). However, to have this transformative role, consent needs to be valid.

386. For decades, a vast literature has highlighted the problems related to consent in the most different areas and, more specifically, as a legitimizing tool for the processing of personal data. In a recent analysis, Solove (2023) maps six main issues, which will be briefly rearranged and summarized below. I will afterwards discuss the specificities of children's consent.

387. The first problem of consenting is related to its formal requirements, its ambiguity and the difficulty of providing evidence that a person *de facto* consented. An invalid consent is an oxymoron, but discussing its validity is an important way to determine the conditions that warrant its transformative role (Kim, 2019-, p. 7). In the case of the GDPR, art. 4 (11) defines consent as “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”. The formal requirements include that it should be freely given, specific, informed, and unambiguous. Even with the requirements that consent should be specific and unambiguous, it is not easy to prove that it was indeed freely given or informed, as will be discussed below.

388. The second issue is related to the substance of one of these requirements: the necessity of consent to be freely given. The information provided to individuals so they can consent is included in privacy policies, in its majority standardized texts with boilerplate language that cannot be negotiated. EDPB Guidance on the issue states that consent is invalid when a data subject “has no real choice, feels compelled to consent or will endure negative consequences if they do not consent [...]” (EDPB, 2020, parag. 13). However, in most of the cases, there is no adequate alternative and not consenting to these unilaterally imposed clauses means to give up of many of the essential services in today's society.

389. Recital 43, GDPR, also takes into account power imbalances and indicates that consent will not be valid in these cases, especially when the controller is a public authority. This is

especially important in the case of more vulnerable data subjects as children, who will likely be in a situation of power imbalance. The educational context is an important example in this regard. The CoE highlights that “children in an educational setting constitute a typical example of a situation where there is an imbalance between the data subject and the controller and where another legal basis should rather be applied” (CoE, 2021, p. 8, footnote 7).

390. Although the GDPR tries to avoid situations of coercion, manipulation is much more difficult to deal with and much less restricted in privacy laws (Solove, 2023). Humans’ rationality is bounded due to their cognitive capacity, time, and access to information. This makes people sometimes to act “irrationally and in ways contrary to their beliefs, desires and self-interest for a variety of reasons” (Kim, 2019-, p. 11). Manipulation techniques are used then to explore these intrinsic human vulnerabilities and, in digital technologies, they are often embedded in their design (e.g. dark patterns) (Hartzog, 2018-). Considering that children are still developing their critical sense and discernment, they are even more easily manipulated, making it crucial to protect their data by design.

391. A third issue concerning using consent as a lawful basis for data processing is the challenge of effectively informing individuals about their choices and the potential impacts. This issue arises for four primary reasons (Solove, 2023). First, making the information available does not mean that people will see it or read it. Second, privacy notices are often excessively lengthy and intricate, filled with legal jargon, which leads to people disregarding them even when they are aware of their existence.

392. Art. 12, GDPR, explicitly states that information must be communicated “in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child”. However, more straightforward notices can end up being vague and not containing important information that could potentially lead to a better understanding of the data processing. Third, being exposed to the information does not mean that people really understand what it means and the risks they are assuming. Finally, incorrect or pre-existing notions that each individual carries will affect how they interpret the terms, and they can end up acting upon false beliefs or inferences about how their data are being processed (Solove, 2023).

393. A fourth problem is the individual’s inability to make decisions (Solove, 2023). When people are in a situation where they need to rapidly decide in order to access something they desire, the cost-benefit analysis can be hampered. While the benefits are often immediate and

concrete (such as accessing a service, a discount, a game, etc.), the risks are difficult to determine. Due to the bias of imaginability, evaluating the predictability of future events is “especially problematic where the future event is novel, unfamiliar or unprecedented. In these situations, the consenting party lacks the experience to make accurate predictions, including the ability to predict his own reactions to the anticipated outcome” (Kim, 2019-, p. 12).

394. To really calculate the costs and benefits, reading and understanding a very lengthy privacy notice would not be enough. One would ideally

know a lot more about the security program that the organization has in place. Does the organization use good encryption? Does it have all the appropriate policies and procedures? Does it train its workforce? Does it adequately vet any vendor that handles personal data or has access to it? To assess confidentiality, the person needs to know about the privacy program. How well-resourced is it? What are the rules for when various types of parties can subpoena the data? How readily and likely will the government access the data? Is the workforce trained about privacy? How are access controls managed? The list can go on and on. Most people end up consenting based on bald statements that data is being protected, but these statements are often boilerplate written by lawyers to sound reassuring without promising very much. People simply do not know enough to meaningfully consent. In most cases, consent means taking a leap of faith in dark (Solove, 2023, p. 31).

395. If it is not possible to understand the full picture and calculate the risks of letting their personal data be processed, then consent cannot be deemed to be informed. Therefore, using consent as a means to exercise individual autonomy and data control in a complex digital environment is often an illusion.

396. The fifth problem revolves around structural limitations related to how consent choices are framed (Solove, 2023, p. 32 et seq.). Some situations involve inadequate, binary choices, where people can either opt in or not. Other situations will involve too many choices, and an approach that is too granular can also be overwhelming. As Kim (2019-, p. 13) argues, more information is not always better, and can “even impair decision-making ability. Psychological studies show that for humans, attention is a scarce resource, and complex information may escape a decision-maker’s notice”. Lastly, and as a consequence of the above, the sixth issue is consent fatigue. When one asks for consent too many times, the actual warning effect of consent mechanism is diminished (EDPB, 2020, parag. 87–88). Even if consent could be informed and freely given, it is difficult to scale.

397. These six issues of consent as a mechanism of individual autonomy and control over one’s personal data are applicable to all data subjects. Nevertheless, children can face even direr challenges. Van der Hof (2017, p. 124–133) uses three lenses based on a rights-based approach to analyze their specificities. First, under a protection lens, although specific rules for children’s

consent are legitimate and even imperative, parents are not necessarily more capable of making these decisions on their behalf. This is mainly because of the facts already enumerated above. From an emancipation and participation perspective, parental consent can also be problematic as it raises tensions between parents and children and can encourage parental surveillance. Especially when it comes to teens, a private space between them and their parents is also essential for their development. In this regard, the GDPR only focuses on one exception in its Recital 38, stating that parental consent “should not be necessary in the context of preventive or counselling services offered directly to a child”.

398. Finally, when viewed through a developmental lens, obtaining consent from children presents significant challenges owing to their varying stages of cognitive and emotional development, coupled with an added layer of vulnerability. Therefore, safeguarding children’s data demands a broader approach beyond merely seeking consent, as it can be seen as a way to free states, private actors and society in general from their responsibility for possible violations (Barret *et al.*, 2021).

399. All the challenges explained above only highlight that the burden of protecting personal data cannot be on children or their parents, and there is a strong need to shift the main responsibility to controllers (Macenaite; Kosta, 2017). In this sense, protecting children’s data will necessarily involve the implementation of high standards of privacy by design (Hof; Lievens, 2018), the establishment of prohibitions on processing certain types of personal data or for certain purposes (e.g. art. 28(2) of the Digital Services Act (DSA), which prohibits processing children’s data for advertisements based on profiling), reframing the role of children’s and parental consent (Solove, 2023), as well as conducting CRIAs alongside Data Protection Impact Assessments (DPIAs).

6.1.4 Other legal bases for processing children’s data

400. Art. 6, GDPR, provides an exhaustive list of legal bases for personal data to be lawfully processed. In order to decide which one is the most appropriate, controllers should consider the impact of the processing on data subjects’ rights, as well as the fairness principle (EDPB, 2019, parag. 1). This includes assessing “the reasonable expectations of the data subjects, considering possible adverse consequences processing may have on them, and having regard to the relationship and potential effects of imbalance between them and the controller” (EDPB, 2019, parag. 12). As consent has been discussed in the previous subsections, I will here focus on the other five legal bases and how they could be applied within the school environment.

6.1.4.1 Contractual necessity

401. Art. 6(1)(b), GDPR, allows the processing of personal data when it “is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract”. In order to use this legal basis, a contract exists must first exist and be valid under the relevant contract law. In the case of children, for example, it is necessary to comply with the age of contractual capacity set by each MS, as well as check the child’s competence to understand what they are agreeing to (DPC, 2021). This age may differ from the legal age of majority, which is currently set at 18 years old in all EU MS. Consequently, unlike consent, the contractual partner does not have the option to revoke their agreement to cease data processing. Instead, the contract would have to be deemed void or terminated in accordance with national contract law (Milkaite, 2021, p. 189).

402. Second, the processing must be necessary for the performance of the contract. This evaluation need to combine a fact-based assessment of the processing for a specific purpose and whether it is less intrusive than other options. If the processing is just beneficial for the controller or included unilaterally in the contract but not objectively indispensable for providing the contractual service, then it is not necessary for the performance of the contract (EDPB, 2019, parag. 25). The principles of purpose limitation and data minimization are particularly important for contracts as they are generally not negotiated on an individual basis within the digital environment (EDPB, 2019, parag. 16).

403. In this context, it is crucial to examine not only the viewpoint of the controller but also that of an average data subject to ensure a genuine mutual understanding of the contractual purpose (EDPB, 2019, p. 32). This becomes particularly pertinent when dealing with children. Even with parental assistance in contracting activities, the child retains their status as the data subject, emphasizing the importance of considering children’s expectations.

404. The necessity criterion requires a strict interpretation, and, based on the accountability principle, the controller must be able to “demonstrate how the main subject-matter of the specific contract with the data subject cannot, as a matter of fact, be performed if the specific processing of the personal data in question does not occur” (EDPB, 2019, parag. 30).

405. In the case of edtech for teaching and learning, the use of this specific legal basis will depend on whether the service is directly provided to children or their parents by the private entity, or if the service is provided by the school. If the relationship is between the private actor and the child or their parents, then some processing activities will probably be necessary for the

performance of this contract. The same applies to the situation where a private school provides the service to a child or their parents based on a contract.

406. Specifically for the purpose of content personalization, as it might be the case for personalized learning, the EDPB is of the opinion that it “may (but not always) constitute an intrinsic and expected element of certain online services, and therefore may be regarded as necessary for the performance of the contract” (EDPB, 2019, parag. 57, emphasis in the original).

407. However, the scenario shifts when a public school delivers a public service, a situation not governed by a private contract. In cases where schools act as the controller or joint controller, they will likely need to seek an alternative legal basis as the only contract that may exist is the one between them and the edtech company, to which the child or their parents are not direct parties.

6.1.4.2 Compliance with a legal obligation

408. Art. 6(1)(c) could be invoked by schools or edtech companies when they must process personal data to fulfil requirements mandated by EU or national laws. It also encompasses situations where the obligation is not defined within a law but rather arise from an additional legal act such as a delegated legislation or binding decision of a public authority. However, it clearly does not cover legal provisions that merely authorize or license something (Kotschy, 2020). To rely on this basis, an organization must be able to pinpoint the precise legal obligation and demonstrate how processing the data is essential for fulfilling it.

409. This is a legal basis which is mostly used by private actors within the educational realm since the public sector will be able to rely on the performance of an official or public task (art. 6(1)(e)). If a public authority is legally obliged to provide education, but the specific means are not defined (such as using digital technologies), the law may not serve as a valid legal basis. In such instances, the authority has ample discretion to determine the manner in which this obligation is met. This lack of specificity would fail to satisfy the binding element for a law to be employed as a legal basis for processing personal data.

410. It is important to mention that the applicability of this legal basis by the public sector had not been entirely ruled out by WP29 in its interpretation of art. 7(c), DPD. However, this provision could only be relied upon when the obligation comes directly from a legislative provision (Kotschy, 2020).

6.1.4.3 Vital interest

411. Using art. 6(1)(d) as a legal basis is less common, as it usually applies to atypical circumstances. Examples would be situations such as “monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters” (Recital 46, GDPR) and other life threats such as when a child is missing or severely ill. Certainly, these situations can be experienced in a school environment. However, in scenarios where elements of urgency and risk or concrete/imminent danger to the data subject’s life are not present, this legal basis is less likely to apply. It could be used in cases of child protection and child welfare measures, for instance.

412. The threshold for fulfilling the necessity element of this legal basis will most probably be lower than when adults’ data are processed, as children are considered to be more vulnerable (DPC, 2021, p. 24). The principle of fair processing may be used as a basis to require that the data subject is consulted when possible (Kotschy, 2020). In the case of children, their right to be heard should be respected as well as their will considering their evolving capacities. It is also important to consider that processing parents’ data may also be necessary to protect the child’s vital interests.

6.1.4.4 Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

413. Art. 6(1)(e) is a general legal basis for the public sector to process personal data. It can be used when data processing is necessary for a task entrusted to the controller¹⁷ to be carried out in the public interest or in exercising official authority. Recital 41, GDPR, clarifies that the EU or national law determining the purpose of processing “should be clear and precise and its application should be foreseeable to persons subject to it”.

414. In contrast to art. 6(1)(c), this provision does not establish specific obligations for the controller. Instead, it grants a broader authorization to take necessary actions to fulfil the assigned task. Based on that, Kotschy (2020, p. 335) argues that art. 6(1)(e) is quite similar to

¹⁷ Kotschy (2020, p. 335) highlights that “[i]n the English version of Article 6(1)(e) it is ambiguous whether the words ‘vested in the controller’ relate to ‘exercise of official authority’ or to ‘a task’. The meaning of Article 6(1)(e) is clearer in the German version where commas are set in order to structure the sentence. Transferring this structure into the English version, it would read as follows: ‘Processing is necessary for the performance of a task, carried out in the public interest or in the exercise of official authority, vested in the controller’. [...] Vesting such a task in a controller requires a legal provision to this effect. Such understanding excludes cases of assignment of ‘tasks’ by contract, even if they were ‘in the public interest’, which will be particularly significant where private entities shall be ‘vested with a task’ in the sense of Article 6(1)(e).”

art. 6(1)(f), as it also demands interpreting and balancing interests. This similarity would probably be the reason why only these two legal bases are subject to the data subject's right to object (art. 21, GDPR).

415. In the case of schools, any activities considered necessary to provide education or to fulfil other obligations related to providing education will likely meet the requirements for using this legal basis as long as they are based on EU or MS legislation. The challenge associated with this legal basis is that the corresponding legal obligations often lack specificity regarding the processing operations they can encompass and the types of data that can be processed for the intended purpose. Consequently, the principle of data minimization serves as a crucial guideline for determining what data are necessary in order to fulfill a specific regulatory requirement.

416. When it comes to the necessity of using edtech, their indispensable utilization was perhaps more evident during the COVID-19 pandemic, when students were learning from home and had to receive education remotely. However, this is less clear in hybrid learning environments.

6.1.4.5 Legitimate interests

417. Based on art. 6(1)(f), GDPR, another possible lawful basis for processing personal data is the legitimate interest of the controller or a third party. It can be used when these interests are not “overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, *in particular where the data subject is a child*”.

418. The concept of legitimate interests is comprehensive and there is no exhaustive list of interests encompassed by it. The GDPR provides some examples in its recitals, such as preventing fraud and direct marketing (recital 47); the transmission of personal data within a group of undertakings for internal administrative purposes (recital 48); or network and information security (recital 49). More generally, *interests* can be defined as “the broader stake that a controller may have in the processing, or the benefit that the controller derives—or that society might derive—from the processing” (WP29, 2014, p. 24).

419. Art. 6(1)(f) calls for a balancing test to assess if the interests of the controller or a third party outweighs the interests or fundamental rights and freedoms of the data subject. Several methodologies have been developed by national DPAs over the years to help controllers carry out this assessment. WP29 provided a list of key steps that should be considered when applying

the balancing test, which includes assessing the particular interest of the controller (if it is a fundamental right, an interest of the wider community or other legitimate interests, as well as the legal and cultural/societal recognition of the legitimacy of the interests); the impact that the processing operation will have on data subjects' interests or fundamental rights (including a risk assessment, the nature of the data, the way data are being processed, the reasonable expectations of the data subject, and the status of the data controller and data subject); carrying out a provisional balance; and applying additional safeguards (such as opt-out mechanisms, immediate deletion of data after being used, anonymization, the use of privacy-enhancing technologies, etc.) (WP29, 2014, p. 33 et seq.).

420. When considering the legitimate interests legal basis, which in general would allow for a proportionate level of interference with data subjects' rights, it is important to adjust the balancing test to the specific situation of children as data subjects (DPC, 2021, p. 25). It cannot be asserted in the abstract that there are no situations where a child's interests cannot be overridden. However, the analysis of the best interests of the child, which include all their fundamental rights enshrined in the CRC, should be a primary consideration when taking a decision that affects them and not just one of the criteria to be weighted.

421. This can be observed when children's data are processed for commercial purposes, such as in profiling, which is suggested to be prohibited by the Committee on the Rights of the Child. Therefore, unless an organization can demonstrate, in accordance with the accountability principle, that profiling children is indispensable to achieve a goal consistent with their best interests, such processing should not proceed.

422. More specifically in relation to the use of the legitimate interests legal basis by schools or edtech, it is important to note that it shouldn't apply to cases in which public authorities perform their official tasks. When it is used by private entities—especially technology companies providing the service directly to a child or in the case of processing operations where they act as a sole controller—this legal basis could be used for example, when measures should be taken or safeguards employed to protect children's health or safety (e.g. processing children's data for the purpose of network safety) (Atabey, 2021).

6.1.5 Analysis of selected data subjects' rights

6.1.5.1 Transparency obligations and the right of access

423. The principle of transparency is further elaborated in arts. 12, 13, and 14 GDPR. According to recital 39, GDPR, natural persons should receive transparent information about the processing of their personal data. It also requires that “any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used”.

424. Art. 12, GDPR, demands that information provided by the controller be “in a concise, transparent, intelligible and easily accessible form, using clear and plain language, *in particular for any information addressed specifically to a child*” (emphasis added). This is reinforced by recital 58, which asserts that “any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand”. This requirement is certainly linked to the right of the child to receive and impart information, enshrined in art. 13, CRC (Milkaite; Lievens, 2020, p. 9). Arts. 13 and 14, GDPR, further list the specific information that should be provided by controllers to data subjects.

425. In relation to children, the way information is provided is crucial for their understanding. Controllers should ensure that “the vocabulary, tone and style of the language used is appropriate to and resonates with children so that the child addressee of the information recognizes that the message/information is being directed at them” (WP29, 2018, parag. 14). Other means of conveying the information apart from text should also be used such as “diagrams, cartoons, graphics, video and audio content, [...] gamified or interactive content [...], privacy dashboards, layered information, icons and symbols to aid children’s understanding and to present the information in a child-friendly way” (ICO, 2020, p. 39).

426. It is essential to also consider the evolving capacities of the child, as the means to inform a younger child should be different from the ones used for teenagers. If many versions of the same information are available, controllers should make all of them “easily accessible and incorporate mechanisms to allow children or parents to choose which version they see, or to down-scale or up-scale the information depending on their individual level of understanding” (ICO, 2020, p. 40).

427. Lastly, it is important to highlight the limitations of providing information to data subjects, especially as a means to allow for more control, as previously discussed. If it is not fair to expect that data subjects understand such intricate processes involving their data, then

the primary burden for protecting personal data should not rest on their shoulders (Milkaite; Lievens, 2020, p. 18). In any scenario, maintaining transparency is of utmost importance, especially as a tool of fostering digital literacy for children.

6.1.5.2 Rectification and erasure

428. Art. 16 stipulates the right to rectification, including not only correction of inaccurate personal data, but also the right to have incomplete data completed. This reflects the principle of accuracy and grants data subjects with more control over the quality of their data (Terwangne, 2020b).

429. In its turn, art. 17 provides data subjects with the right to erasure (“right to be forgotten”), where specific grounds should be identified. Three of these grounds are related to the lack of basis for the processing (personal data are no longer necessary; consent had been withdrawn; personal data are unlawfully processed). The others demand erasure as a consequence of the right to object (art. 21), the compliance with a legal obligation, and the collection of data when the data subject was a child and consent has been given by the holder of parental responsibility (art. 8(1)).

430. Recital 65 emphasizes that the right to erasure is particularly important in cases where the data subject was a child when the consent had been given and was not fully aware of the risks associated with the processing. This right can be exercised even when the data subject reaches adulthood. Some scholars view the right to be forgotten as the most prominent empowering right in the GDPR (Macenaite, 2017), as it not only provides children with the right to remove information about them that could be damaging to their reputation but also information that is no longer relevant with the passage of time (Haley, 2020).

431. It must be recognized, however, that this right has several limitations. It only applies to the situations where consent was adopted as a legal basis—which is increasingly rarer—(unless other items in paragraph 1 apply), and the processing is not necessary for the purposes listed in paragraph 3. It remains a crucial right, though, particularly in cases where the child disagrees with the consent provided on their behalf and wishes to delete the data in the future, regardless of their reason. It is important to recall that while the holder of parental responsibility exercises this right on behalf of the child, the child remains the ultimate rights holder and should have the opportunity to reassess these decisions when they become capable of doing so.

432. Apart from art. 16 and 17, it is important to mention the more adjunct rights laid down in arts. 18 and 19. Art. 18 sets forth the right to the restriction of process, which permits the temporary limitation of processing until specific rights are granted, serving as a measure to hinder processing that would otherwise be deemed lawful (González Fuster, 2020). Art. 18 can then be used when the data subject claims that their data are not accurate, during the period in which the controller verifies the data; when the processing is unlawful, and instead of erasure, the data controller requests restriction; when the controller no longer needs the data for the intended purpose, but the data subject requests restriction in order to exercise or defend legal claims; and when the right to object has been exercised, during the period in which the analysis under art. 21(1) is conducted. Conversely, under art. 19, controllers need to notify data recipients with whom they have shared the data that a rectification, erasure or restriction of process has been carried out.

6.1.5.3 Right to data portability

433. Data portability is a very important right when it comes to changing schools. Laird and Quay-de la Valle (2019) note that student mobility is often associated with disengagement, increased dropout rates, and lower educational achievements. Challenges related to data portability could contribute to these issues. For instance, the absence or poor execution of data portability may lead to delayed student enrollment, incorrect class placement, discontinued special services (such as for students with disabilities) and lack of security (such as in cases of food allergies) (Laird; Quay-de la Vallee, 2019).

434. Although rooted in competition concerns, the right to data portability under the GDPR is also meant to empower data subjects. According to art. 20, individuals have the right to receive their personal data provided to the data controller (i.e., data knowingly and actively provided by the data subject or observed data) in a structured, commonly used, and machine-readable format.

435. The scope of this right is limited to data which are processed based on consent or contract, which, as previously observed, are used quite scarcely in the educational domain when it comes to public education. The situation differs in private schools, where a substantial portion of student data is processed based on the contract established between the two parties. Recital 68 and art. 20(3) emphasize that data portability will not apply when the data processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Nevertheless, WP29 guidelines on the matter

(endorsed in 2018 by the EDPB) suggests that it is a good practice. Data portability within the school environment is also very often regulated by specific laws in each EU MS.

436. Restricting data portability to data that are provided by the data subject can also be a challenge, especially when personalized learning activities are in place. The lack of context or insufficient data could hinder the right to education and lead to incorrect decisions. WP29 clarifies that data should be provided to the data subject along with relevant metadata at a suitable level of granularity to accurately describe the information's meaning and facilitate its function and reuse (WP29, 2017, p. 18). At the same time, oversharing information, especially without context, could enhance biased decision-making and create social stigma. For instance, a student with a history of disciplinary measures might face issues in the new school if the context that the issues were a result of persistent bullying is also not shared (Laird; Quay-de la Vallee, 2019, p. 8).

6.1.5.4 Right to object

437. Enshrined in art. 21, GDPR, the right to object refers to the data subject's ability to request that the processing activities stop according to his or her particular situation. Art. 21(1) lays down a more general right to object, which must be aligned with certain requirements, while art. 21(2) refers to an unconditional right to object when the data are processed for direct marketing.

438. The general right to object applies only when the data has been processed based on the necessity for a task in the public interest or in the exercise of official authority vested in the controller, or on the legitimate interests of the controller (art. 6(1)(e) and (f)). This is an particular right as it demands a balance test of its own (beyond the *ex-ante* balancing test performed when processing based on 6(1)(e), for example) and, therefore, is a manifestation of the fairness principle (Ausloos, 2017).

439. When data subjects object to the processing of data, they cannot be processed anymore, unless the controller has compelling legitimate grounds not to do so—i.e., grounds that overwhelmingly override the interests, rights, and freedoms of the data subject—or needs the data to exercise or defend legal claims. The burden of proof lies with the controller to assess the interests at stake and prove that their interest compellingly overrides the ones of the data subject.

440. Understanding what can be considered compelling legitimate grounds is crucial, since all processing based on art. 6(1)(f) already has to pass through a balancing test. If the legitimate interest merely overrides that of the data subject, there would not be a situation where the latter could object (Zanfir-Fortuna, 2020). When it comes to processing activities based on art. 6(1)(e), however, this stricter balancing exercise is not mandatory (although, of course, the principles of necessity and proportionality should always apply) and would need to be done if the data subject objects to the processing activity.

441. Regarding the burden of proof, it rests on both the controller and the data subject, albeit with the former bearing a more substantial responsibility. The accountability principle requires the controller to conduct a prior analysis of the appropriate legal basis before data processing begins. In the case of processing based on legitimate interests, a balancing exercise must be undertaken under the controller's burden of proof. However, if this analysis is challenged, the data subject is required to substantiate their claim (Ausloos, 2017).

442. Since these two legal bases are commonly used in educational settings for data processing related to teaching and learning, the right to object holds significant importance for children. Considering the unique circumstances of being a child in the digital environment, as elaborated in Chapter 4, it may already satisfy the condition of the data subject's "particular situation".

443. With regards to justifying the data processing based on legitimate interest, it can be argued that the principle of best interests would inherently elevate the standard in terms of the necessary balancing test, and the controller's interest would need to substantially outweigh the child's interest. However, this is not the case for art. 6(1)(e). Although the principle of the best interest should necessarily apply to all decisions concerning a child and, therefore, to the processing of their data, this specific right grants children a direct method to enforce it after the data processing has started.

444. Upon its application, it compels schools or other institutions that may process their data under art. 6(1)(e) to conduct a balancing test. This is endorsed by the Committee on the Rights of the Child (2021, parag. 72), which in its General Comment 25 states that children should be ensured the right to "object to personal data processing where the data controller does not demonstrate legitimate, overriding grounds for the processing", especially when this could be seen as surveillance in the educational setting (parag. 75).

445. One example could involve the processing of personal data for the purpose of personalizing learning. Such processing could indeed be perceived as a way to uphold children's rights to education and lawful under the GDPR. Nevertheless, depending on the specific use case, if a child or their parents perceive that this process would encroach upon their right to privacy or non-discrimination, they could make use of the right to object to cease the processing. The school would, therefore, be required to conduct a balancing test and provide an alternative service if their legitimate grounds does not outweigh the rights of the child.

6.1.5.5 Automated individual decision-making

446. Art. 22, GDPR, gives data subjects the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or similar significant effects on them. Unlike the DPD, this article includes not only profiling, but also other types of automated decisions. In practice, however, most types of automated decisions which fall under the scope of art. 22 will likely include profiling (Bygrave, 2020b). Although worded as a right, the WP29 was of the opinion that it establishes a general prohibition for decision-making based solely on automated processing in certain circumstances. This opinion was endorsed by the EDPB (EDPB, 2018) and very recently confirmed by the CJEU (European Union, 2023).

447. When it comes to profiling, art. 4(4), GDPR, defines it as encompassing two processes. First, it involves inferring the characteristics of an individual or group (creating a profile). Second, it involves interacting with that individual or group based on those attributes (employing the profile). The GDPR definition, however, narrows down this scope to automated processing of personal data (Bygrave, 2020a).

448. Recital 71, GDPR, provides details on automated decision-making based on profiling with legal or similarly significant effects and states, at the end, that this *should not concern a child*. At first, this could lead to the understanding that being a child, in itself, would be enough for decisions based solely on automated processing to meet the significant effects threshold (Bygrave, 2020b, p. 534). This means that human intervention should always be employed when dealing with children's data.

449. However, it could also mean that decisions based on automated processing concerning children could be carried out, as long as it does not produce any legal effects for or similarly significantly affects the child (Lievens; Verdoodt, 2018, p. 276). Given that the legislator likely included this phrase for a specific purpose, particularly considering that the rule already applies

to all data subjects, it is essential to analyze Recital 65 in its entirety and examine its interconnection with other recitals to gain a comprehensive understanding.

450. Regarding the structure of the recital itself, it first states that data subjects have the right not to be subject to a decision, which may include profiling, based solely on automated processing and which produces legal effects or similarly significantly affects them. After providing some examples and explaining the definition of profiling, the recital includes exemptions when this kind of decision-making is allowed and appropriate safeguards that should be implemented. Only then, it says that such measures should not concern a child. Therefore, this could be interpreted in a way that the exemptions would not be applicable to children.

451. Recital 38 also clarifies that a specific protection for children's data would, "in particular, apply to the use of personal data of children for the purposes of marketing or *creating personality or user profiles* and the collection of personal data with regard to children when using services offered directly to a child". This reinforces this second interpretation, as it foresees profiling as a possibility.

452. This second view is also supported by the Committee on the Rights of the Child (2021), which demands that states ensure that "automated processes of information filtering, profiling, marketing and decision-making do not supplant, manipulate or interfere with children's ability to form and express their opinions in the digital environment" (para 61) or are used to affect or influence children's behavior or emotions or to limit their opportunities or development (para 62).

453. WP29 was of the opinion that this could not be interpreted as a prohibition because it is stated in a recital, which is not binding. However, it recommended that, "as a rule, controllers should not rely upon the exceptions in Article 22(2) to justify it" (WP29, 2016, p. 28). An exception would be when "solely automated decision-making, including profiling, with legal or similarly significant effects in relation to children [... is used] to protect their welfare. If so, the processing may be carried out on the basis of the exceptions in Article 22(2)(a), (b) or (c) as appropriate" (WP29, 2016, p. 28).

454. In any scenario, one could argue that automated decisions based on profiling in the educational setting would indeed fall within the scope of what constitutes a legal or similarly significant effect. In terms of legal effects, it could hinder the right to education, when it is used for providing access to educational institutions or for assessing students. When it comes to

similarly significant effects, recital 71 mentions the example of e-recruiting practices without human intervention, which could also use educational data.

455. WP29 (2016, p. 21) defines what can significantly affect individuals as the decisions that have the potential to: “significantly affect the circumstances, behaviour or choices of the individuals concerned; have a prolonged or permanent impact on the data subject; or at its most extreme, lead to the exclusion or discrimination of individuals”. As described throughout this thesis, it can be argued that all these three situations could result from automated decisions based on profiling within the educational realm, which emphasizes the need for having human intervention at all times.

456. Specifically in relation to targeting advertisement, WP29 emphasized that “data controllers should not process children’s data for behavioral advertising purposes, neither directly nor indirectly, as this will be outside the scope of a child’s understanding and therefore exceed the boundaries of lawful processing” (WP29, 2013, p. 26). The EDPB reiterated this idea in the endorsed guidelines on automated individual decision-making and profiling, stating that organizations should refrain from profiling children for marketing purposes (WP29, 2016). More recently, art. 28(2) of the DSA has introduced a prohibition on online platforms, barring them from displaying advertisements targeted at minors through profiling.

6.1.6 Data Protection Impact Assessment (DPIA)

457. Under the accountability principle, controllers are required to demonstrate compliance with the GDPR, considering “the risks of varying likelihood and severity for the rights and freedoms of natural persons” (art. 24(1), GDPR). For certain kinds of processing activities that are “likely to result in a high risk to the rights and freedoms of natural persons” (art. 35(1), GDPR), the GDPR mandates the undertaking of a DPIA.

458. The DPIA is “designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them” (WP29, 2017, p. 4). The operative text of the GDPR *per se* does not explicitly consider the processing of children’s data as carrying a high risk (Hof; Lievens, 2018, p. 17). However, recital 75 explains that when personal data of vulnerable natural persons, such as children, are processed, this may result in risk to their rights and freedoms. WP29 also considered that the processing of data from vulnerable data subjects should be considered as one of the criteria

evaluated by the controller in order to determine if a DPIA should be undertaken “because of the increased power imbalance between the data subjects and the data controller” (WP29, 2017, p. 10).

459. It is also important to highlight the role of the principle of the best interest of the child as rule of procedure, that requires an evaluation of the positive or negative impacts of a decision on the child in every decision-making process that could affect them (Committee on the Rights of the Child, 2013a, parag. 6). Since several of the rights recognized by the CRC may be affected when processing children’s data, it is crucial to perform a child rights-oriented DPIA (Hof; Lievens, 2018, p. 19) and leverage methodologies that already exist for CRIAs.

6.2 AI Act

460. At the time of completing this thesis, the EU Council and Parliament have reached an agreement on the AI Act (Council of the European Union, 2023a). As the final text is not yet available for analysis, I will use this section to provide a high-level overview of the fundamental ways in which the AI Act (European Union, 2021), as subjected to the analysis of the Committee of Permanent Representatives (COREPER) on 26 January 2024 (Council of the European Union, 2024), may impact the use of edtech. A thorough analysis of the impacts of the AI Act on edtech and on children’s data protection will be essential once the final text becomes available, and this is intended to be carried out elsewhere.

461. The AI Act proposal was announced in April 2021 and aimed to be a technology-neutral, cross-cutting EU legislative instrument setting rules for the development, placing on the market, and use of AI products and services. The proposal was linked to many other policy and investment initiatives, such as the White Paper on Artificial Intelligence (European Commission, 2020d); the Communication on Fostering a European approach to Artificial Intelligence (European Commission, 2021b); the Coordinated Plan on AI (European Commission, 2021c); as well as the Horizon Europe and Digital Europe programs (European Commission, 2021a, n.p.). It is important to mention that the AI Liability Directive (European Commission, 2022b) is also intrinsically linked to the AI Act, but will not be discussed in this thesis.

462. Based on arts. 114 and 16 of the TFEU, the main purpose of the regulation is to ensure the harmonization and proper functioning of the single market, preventing fragmentation and providing legal certainty (recitals (1) and (2)). Recital 1 also emphasizes its aim to

promote the uptake of human centric and trustworthy artificial intelligence while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy and rule of law and environmental protection, against harmful effects of artificial intelligence systems in the Union and to support innovation.

463. The regulation also supports the objective of the EU to become a global leader in the development of secure, trustworthy and ethical artificial intelligence.

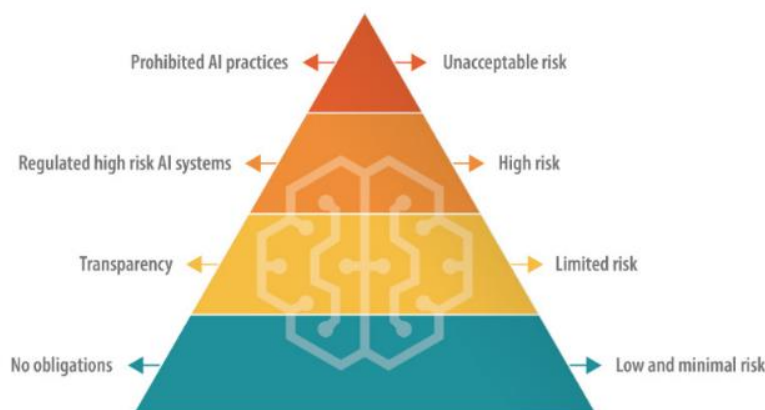
464. It applies to all AI systems impacting people in the EU, across all sectors, and contains certain extraterritorial measures affecting AI systems that impact people within the EU. The definition of AI system was aligned with the recently updated definition used by the OECD:

[a]n AI system is a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

465. The AI Act adopts a tiered risk-based approach, whereby different obligations are defined according to the legal, economic and ethical risks that AI systems can pose to society. Recital 14a recalls, however, the 2019 Ethics Guidelines for Trustworthy AI and its seven non-binding ethical principles for AI, emphasizing their role in promoting trustworthy and ethically sound AI.

466. As shown in the figure below and explained in its recital 14, the AI Act distinguishes between a) unacceptable risk—which are banned—b) high risk—which are more heavily regulated by a new set of obligations—c) limited risk—which are subject to a set of transparency rules—and d) low or minimal risks—which could be freely developed and used in the EU. General-purpose AI (GPAI) systems follow a separate framework which will be discussed below.

Figure 3 - AI Act risk-based approach - pyramid of risks



Source: Madiega (2023, p. 4)

467. Title II establishes a list of prohibited AI, which includes practices that have a significant potential to manipulate persons through subliminal techniques beyond their consciousness; exploit vulnerabilities of specific vulnerable groups, including due to their age, disability or a specific social or economic situation; and infer sensitive data through biometric categorization. More specifically related to edtech, it prohibits the use of AI systems to infer emotions in educational institutions, except when put in place or into the market for medical or safety reasons.

468. Title III lays down specific requirements for what is considered high-risk AI, which carries most of the compliance obligations within the AI Act. Instead of providing a definition of what is considered high risk, the AI Act provides a list of these systems in its art. 6 and Annexes II and III. The Commission retains the possibility of expanding this list in the future as long as some specific conditions are met. No explanation has been provided as to why these specific systems and not others are listed. Moreover, no analysis has been carried out to assess whether the high risks posed by these systems are necessary and proportionate according to art. 41, CFR.

469. Included in the lists are AI systems used as safety components or a product covered by EU harmonization legislation, such as medical devices, motor vehicles and civil aviation. Annex III also includes different contexts where AI systems are applied, posing significant risk of harm to health, safety, or fundamental rights.

470. Recital 28a explains that the adverse impacts caused by the AI system on the fundamental rights protected by the Charter are of particular relevance when classifying an AI system as high-risk. More specifically, the recital highlights that

children have specific rights as enshrined in Article 24 of the EU Charter and in the UN Convention on the Rights of the Child (further elaborated in the UNCRC General Comment No. 25 as regards the digital environment), both of which require consideration of the children's vulnerabilities and provision of such protection and care as necessary for their well-being.

471. In this regard, two of the categories within Annex III are relevant to this thesis. First, it includes some AI systems used for education and vocational training, i.e., AI systems intended to be used to determine access or admission or to assign natural persons to educational and vocational training institutions at all levels; AI systems intended to be used to evaluate learning outcomes, including when those outcomes are used to steer the learning process of natural persons in educational and vocational training institutions at all levels; AI systems intended to be used for the purpose of assessing the appropriate level of education that individual will

receive or will be able to access, in the context of/within education and vocational training institution; and AI systems intended to be used for monitoring and detecting prohibited behavior of students during tests in the context of/within education and vocational training institutions.

472. Recital 35 explains that these systems should be considered high-risk because they

may determine the educational and professional course of a person's life and therefore affect their ability to secure their livelihood. When improperly designed and used, such systems may violate the right to education and training as well as the right not to be discriminated against and perpetuate historical patterns of discrimination.

473. The comprehensiveness of AI systems mentioned under this category of Annex III is welcomed and would encompass most the technologies mentioned by this thesis.

474. In Annex III of the AI Act, another significant category of AI systems pertains to accessing and enjoying essential private services and public services and benefits, which could include educational services. While access to education is already covered by a specific category, the addition of the term “enjoyment” holds particular importance in the context of education. This inclusion encompasses systems such as student behavior monitoring and other edtech that could potentially impact the complete enjoyment of the right to education beyond monitoring and detecting prohibited behavior. Additionally, AI systems used in employment settings are pertinent, encompassing recruitment systems that may process personal data gathered during a child's school years.

475. There are some exceptions to this high-risk classification. AI systems will not be considered high-risk, based on art. 6(2a), if they are intended to perform a narrow procedural task; improve the result of a previously completed human activity; detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or perform a preparatory task to an assessment relevant for the purpose of the use cases listed in Annex III.

476. In relation to the obligations established by the regulation for high-risk AI systems, art. 9 mandates the establishment of a risk management system, which should be understood as a continuous iterative process, planned and run throughout its entire lifecycle (art. 9, (2)). It must comprise a series of steps, such as identification and analysis of the known and reasonably foreseeable risks; estimation and evaluation of the risks that may emerge; evaluation of emerging risks based on post-market monitoring; and the adoption of appropriate and targeted risk management measures designed to address the risks identified in the previous steps. The risk management system should not only consist of documentation, but also of a testing phase

according to art. 9(5). Art. 9(8) also determines that when implementing the risk management system described in paragraphs 1 to 6, specific consideration shall be given to whether the high-risk AI system is likely to be accessed by or have an impact on children.

477. The risk management system is then at the core of the AI Act approach. The quality and comprehensiveness of the identification and classification of the risks will set the tone for the mitigation measures that will be implemented. The AI Act leaves, however, a lot of discretion to the AI provider in determining which measures must be taken to deal with the identified risks and at which point they are considered enough (Smuha *et al.*, 2021). According to art 9(4), the provider will have to determine what is a relevant residual risk and if the measures taken are enough to make them reasonably acceptable. The residual risks should be communicated to the deployer.

478. It is commendable that children's specificities have been included in this provision. However, considering their vulnerability, it does not seem appropriate for actors who will themselves face the consequences of enforcement to determine the required mitigation measures and what qualifies as an acceptable yet relevant risk. If a provider intends to introduce a product to the market or into service within the EU, it is unwise to assume that they could act in a way that might conflict with their commercial interests. At the very least, stakeholders who are subject to the AI system, particularly children who have the right to be heard, should be consulted about what level of risk may be considered acceptable (Smuha *et al.*, 2021). Children also have the fundamental right to have their interests taken into consideration in every decision that affects them, and we cannot be sure if this will be the case with this procedure, especially because the results would be only shared with the user (art. 9(4)).

479. General obligations related to high-risk AI systems include implementing appropriate data governance and management practices for training, validating and testing data sets to be used in AI systems. These practices must consider, for example, design choices and possible biases that can negatively impact fundamental rights or lead to prohibited discrimination. Data sets are also required to be sufficiently representative, free of errors, and take into account the geographical, contextual, behavioral or functional setting within which the system is intended to be used.

480. These are very important requirements to be considered when it comes to edtech, especially due to their capacity to limit children's opportunities in life. However, some challenges still remain in their application, especially due to the broad discretion that AI

providers enjoy, as explained above when faced with open expressions such as “appropriate” and “sufficiently representative”. Moreover, the provider is not necessarily in a good position to define the broader context in which the system will be deployed so it could be taken into account when gathering the data set. Since AI is an umbrella term for different technologies, context makes a tremendous difference in the risks they pose (Smuha, 2023b).

481. Other obligations include maintaining technical documentation and record-keeping; being transparent and providing information to users; enabling and conducting human oversight; and complying with standards for accuracy, robustness and cybersecurity. High-risk AI systems must also be as resilient as possible regarding errors, faults or inconsistencies.

482. Deployers of high-risk AI systems must also comply with certain obligations, such as carrying out a fundamental rights impact assessment (FRIA) if they are a public body or private entity providing public services; implementing human oversight; ensuring that input data is relevant to the use of the system, among others. This would be the case of schools, for example, that deploy AI systems for the purposes established in point 3 of Annex III.

483. Finally, for certain AI systems that are not prohibited nor considered high-risk, the AI Act establishes transparency obligations (Title IV). For example, AI systems intended to interact with natural persons should be designed and developed in such a way that people are informed that they are interacting with an AI system. Companies developing such systems are also invited to commit to codes of conduct on a voluntary basis.

484. When it comes to GPAI¹⁸, the AI Act also adopts a tiered approach, differentiating between high-impact GPAI with systemic risk and other GPAI models. The latter should comply with limited transparency obligations, such as keeping up-to-date and making available, upon request, technical documentation, as well as providing certain information and documentation to downstream providers for the purpose of compliance with the AI Act. The former should also perform model evaluation; make risk assessments and take risk mitigation measures; ensure an adequate level of cybersecurity protection; and report serious incidents to the AI Office and national competent authorities.

¹⁸ According to art. 3(44b) of the AI Act, “‘general-purpose AI model’ means an AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable to competently perform a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications. This does not cover AI models that are used before release on the market for research, development and prototyping activities.”

485. The AI Act is expected to be approved by the European Parliament and the Council and published in the Official Journal in early 2024. The current agreement foresees a phased timeline for enforcement, starting with prohibited AI systems and progressively extending to other AI systems until 2028.

6.3 EU policy on digital education

486. According to art. 165, TFEU, the primary responsibility for education lies with EU MS, leaving the EU with only a supporting role. The Commission believes that education is the “foundation for personal fulfilment, employability and active, responsible citizenship” and “is essential to the vitality of European societies and economies” (European Commission, [s. d.], n.p.) A European Education Area would thus help MS develop education and training systems that are more resilient and inclusive (European Commission, [s. d.]).

487. At the 2017 Social Summit in Gothenburg, Sweden, European leaders first endorsed the idea to create a European Education Area (European Commission, [s. d.]). Between 2017 and 2020, the Commission has taken three important steps to lay down its vision for its establishment (Chircop, 2021).

488. First, in November 2017, it issued the Communication “Strengthening European Identity through Education and Culture” (European Commission, 2017c) as its contribution to the Summit. The Commission identifies several challenges in the areas of education and culture, including digitization, automation, artificial intelligence, as well as the future needs for specific skills and competences. Therefore, it sets out the vision of a European Education Area—building on the New Skills Agenda for Europe (European Commission, 2016a), as well as investing in Europe’s youth initiatives (European Commission, 2016c, 2016b, 2017b, 2017a)—as a “driver for jobs, social fairness, active citizenship as well as a means to experience *European identity in all its diversity*” (European Commission, 2017c, n.p., emphasis in the original). The solutions identified by the Commission encompassed mutual recognition of diplomas, boosting the Erasmus+ program, defining benchmarks for digital competences and lifelong learning, and “prepare a new *Digital Education Action Plan* in order to *promote innovative, personalised and digital teaching methods* and technologies that will help improve learning outcomes” (European Commission, 2017c, n.p., emphasis in the original).

489. Two months after the Summit, in January 2018, the Commission launched three initiatives to improve key competences and digital skills of European citizens, and to promote

common values and pupils' awareness of the functioning of the EU (European Commission, 2018c). The proposals fed into the first European Education Summit. The initiatives included two Council Recommendations on key competences for lifelong learning (Council of the European Union, 2018a), and on common values, inclusive education and the European dimension of teaching (Council of the European Union, 2018b). A third initiative was the Digital Education Action Plan (DEAP)—which outlined ways to make better use of digital technology for teaching and learning; develop the digital competences and skills needed for living and working in an age of digital transformation; and improve education through better data analysis and foresight (European Commission, 2018b).

490. Another package of measures in 2018 was described by the Communication “Building a stronger Europe: the role of youth, education, and culture policies” (European Commission, 2018a). This communication highlighted that 44% of Europeans were still considered to have low or no digital skills and that more attention needed to be devoted to education, training and culture to unlock their full potential to support the European project (European Commission, 2018a, p. 2). The Commission then announced the Youth Strategy, the New European Agenda for Culture, and three proposals for Council Recommendations on “Mutual Recognition of Diplomas”, improving the “Teaching and Learning of Languages” and on “High Quality Early Childhood Education and Care Systems”.

491. Finally, a third communication of 2020 set out the vision to achieve the European Education Area by 2025 and presented more concrete steps to deliver it (European Commission, 2020c). It was followed by two Council resolutions in 2021 on a strategic framework for European cooperation in education and training towards the European Education Area and beyond (2021-2030) (Council of the European Union, 2021a) and on the strategic framework's governance structure (Council of the European Union, 2021b).

492. As part of the European Education Area enabling framework, the first DEAP (2018-2020) was important in promoting cooperation and dialogue on digital education. However, due to its short duration and limited budget, the actions' full potential and expected impact could not be achieved, according to the Commission (Binder, 2023; European Commission, 2020a). A second DEAP (2021-2027) was then adopted in September 2020 (European Commission, 2020b) and, in comparison to the 2018-2020 action plan, this DEAP has a lengthier duration, lasting from 2021 to 2027 and a more expansive scope, as it also encompasses informal and non-formal education, based on a lifelong learning approach (Binder, 2023).

493. The plan understands that there are two aspects that need to be focused on when it comes to digital education. First, it is necessary to assess the deployment of the vast and growing array of digital technologies. Second, there is the need to equip learners with digital competences (knowledge, skills and attitudes). The priority areas set out by this DEAP are: 1) Fostering the development of a high-performing digital education ecosystem; and 2) Enhancing digital skills and competences for the digital transformation. The DEAP also highlights some guiding principles, which include that digital education should be high quality, and protect personal data and ethics (European Commission, 2020b).

494. The development of a high-performing digital education ecosystem has several layers, and they are reflected in the actions outlined under this area. A very important one involves ensuring proper access to internet connectivity and digital technology. On average, 5% of European children lack access to computers at home. Although this percentage may initially appear small (especially when compared to Brazilian children), significant disparities exist among MS. For example, while only 0.7% of Estonian children face this issue, the figure rises dramatically to 23.1% for Romanian children (Niestadt, 2022).

495. Action 4, therefore, help reduce these disparities by supporting Gigabit connectivity and 5G coverage in certain areas and action 5 aims at supporting teachers on developing their digital competences (Binder, 2023). Finally, the development of ethical guidelines on the use of AI and data in teaching and learning for educations was also part of the first area as per action 6.

496. The second area directly supports the Skills Agenda, as it establishes objectives related to the uptake of digital competences. It includes the creation of a common European Digital Skills Certificate (EDSC) and the uptake of the European Digital Competence Framework to include AI and data skills (Muraille, 2020).

497. The implementation of the DEAP is synergetic with several other EU initiatives. It supports the European Skills Agenda (European Commission, [s. d.]) by ensuring that 70% of 16 to 74-years-olds have at least basic digital skills by 2025. The European Year of Skills 2023 seeks to strengthen synergies between skills policies and EU initiatives on training, such as the DEAP and the European Education Area (European Parliament; Council of the European Union, 2023). When it comes to the 2030 digital compass and the Digital Decade policy program (European Commission, [s. d.]), the plan helps implementing the goal of a digitally skilled population and highly skilled digital professionals. It also supports the Commission's "A Europe fit for the digital age" (European Commission, [s. d.]) priority, contributes to the

Next Generation EU (NGEU) recovery instrument (European Commission, [s. d.]), and is related to the new European Strategy for a better internet for kids (BIK+).

498. Finally, it is also important to mention the development of a Data Spaces for Skills within the Data Strategy. In addition to foreseeing the issuing of new legislation such as the Data Governance Act (DGA) and the Data Act (DA), the Data Strategy also includes investment in common European data spaces in strategic sectors through the Digital Europe Programme. According to the Data Spaces Support Centre (DSSC) (2023, p. 6), a data space is “a distributed system defined by a governance framework, that enables trustworthy data transactions between participants while supporting trust and data sovereignty. A data space is implemented by one or more infrastructures and supports one or more use cases.”

499. The Data Space for Skills would then be a framework for sharing data related to qualifications, learning opportunities, jobs and skills. The purposes for the data sharing include

analytical and statistical purposes to policy development or reuse in innovative applications, as well as at providing easy, cross-border access to key datasets. The European skills data space will also aim to reduce the skills mismatches between education and training systems on the one hand and labour market needs on the other. Besides improving skills intelligence, this data space will deliver services to its users, with recommendations of learning opportunities to support their upskilling efforts, tailored to the information on their skills profiles (European Commission, 2022a, p. 32–33).

500. Considering the novelty of the concept of data spaces and the fact that they are still ill-defined, the full array of effects this may have on children’s rights are still unknown. The benefits of a large amount of data “on the market” for fundamental rights are not adequately proven. However, it is already well-known that widespread data sharing can have serious consequences for protecting personal data and, consequently, other fundamental rights. The data strategy may be reinforcing a narrative of commodification of personal data which might contradict the main aim of the GDPR to protect fundamental rights. It could also affect children’s rights not to be subject to economic exploitation.

501. The interplay and overlap between the data strategy and the new data regulation with the GDPR is also still not fully assessed, and new conflicts can arise while implementing them. An area of potential friction between the objectives of the strategy and the GDPR lies, for example, in the principles of purpose limitation and data minimization (Fernandes; Sas, 2023). While the goal of the creation of a data space is to make data available for further use, these principles should be, according to the WP29, interpreted more strictly when it comes to children (WP29, 2013).

Chapter 7. Brazil's relevant legal frameworks

502. Before the enactment of the LGPD (Brasil, 2018b))¹⁹ in 2018, which marked Brazil's first data protection law, its legal framework contained some data protection rules scattered across various regulations. They were included, for instance, in the Internet Bill of Rights (Brasil, 2014), the Consumer Protection Code (Brasil, 1990), the Access to Public Information Law (Brasil, 2011a), the Civil Code (Brasil, 2022a), the Good Payer's Registry Law (Brasil, 2011b) and Interception of Telephone Communication Law (Brasil, 1996).

503. This patchwork of legal frameworks proved insufficient to adequately safeguard the rights of data subjects. For many years, various stakeholders advocated for a comprehensive data protection law. The development of LGPD was significantly influenced by Convention 108 of the CoE, the DPD, and the GDPR. Similar to the GDPR, LGPD applies to both the public and private sectors, employs an ex-ante protection system, and emphasizes the accountability approach. It establishes a minimum set of principles and rights for data subjects, which must be adhered to in all personal data processing activities and requires a legal basis for data processing.

504. The enforcement of LGPD falls under the purview of the National Data Protection Authority (*Autoridade Nacional de Proteção de Dados – ANPD*). Originally conceived as an independent body, the creation of this new agency in Brazil was deemed unconstitutional by the president of the republic at the time. The Presidency argued that only the executive branch had the authority to establish such an entity. Consequently, while the president sanctioned the LGPD, it vetoed the provisions related to the ANPD and immediately after issued Provisional Measure (Medida Provisória - MP) No. 869/2018²⁰, which positioned the ANPD as an entity subordinate to the Presidency of the Republic. This move eliminated the financial and political autonomy of the authority. The ANPD only began its operations in November 2020, following the appointment of its first directors.

505. In 2022, another MP altered the LGPD and transformed the ANPD into a “special nature autarchy” (Brasil, 2022b), granting it autonomy and independence in its decision-making and normative publications. More recently, a Presidential Decree linked the ANPD to the Brazilian

¹⁹ For an English translation of the law, see Lemos *et al.* (2020).

²⁰ Transformed into Law n. 13.853/2019 (Brasil, 2019).

Ministry of Justice and Public Safety, thus ending its direct affiliation with the Presidency of the Republic (Brasil, 2023a).

506. The Brazilian Federal Constitution (*Constituição da República Federativa do Brasil – CRFB*) (Brasil, 1988) also contains significant provisions for the protection of personal data. It provides for the right to privacy in its art. 5º, X; the right to the secrecy of correspondence in its art. 5º, XII; and the *habeas-data* in art. 5º LXXII, a constitutional remedy that guarantees individuals the right to know whether a public entity is processing their data and, if necessary, the subsequent rectification.

507. Since 2020, data protection has been recognized as a fundamental right in Brazil, following a landmark decision by the Brazilian Supreme Federal Court (*Supremo Tribunal Federal – STF*). In 2022, the Constitution was amended to include the right to the protection of personal data as a fundamental right in the Brazilian legal order (art. 5º, LXXIX), separate from the right to privacy. This provision also grants an exclusive federal competence to organize, oversee and draft bills on the right to the protection of personal data and data processing.

7.1 The Brazilian General Data Protection Law (LGPD)

508. This section outlines specific issues that affect the processing of children’s data according to the LGPD, particularly within the school environment. Due to the significant similarities between the GDPR and the LGPD, many of the comments made in the context of GDPR remain valid. Therefore, to avoid redundancy, I will strive to elaborate on the similarities and differences between the laws in each section and provide commentary only on the aspects that differ.

509. The LGPD is a horizontal law, applicable to both the public and private sectors. The exceptions for application are limited and provided for in its art. 4º. The law establishes the foundations and principles of personal data protection, an exhaustive list of applicable legal bases, important definitions, obligations for controllers and processors, as well as rights for data subjects.

7.1.1 General Principles for Data Processing

510. While the GDPR provides seven principles for data processing, the LGPD offers eleven. Apart from minor differences in the wording of the provisions, the principles contained in both

laws are purpose limitation; data minimization and storage limitation (both covered by the principle of necessity, in LGPD); accuracy (data quality, in LGPD); integrity and confidentiality (security, in LGPD); and accountability. The principle of lawfulness, fairness and transparency, in the GDPR, is encompassed by several other principles in LGPD, namely adequacy (compatibility of the processing with the purposes informed to the data subject, according to the context of the processing), prevention (adoption of measures to prevent harm due to the processing of personal data), good faith and transparency. LGPD also includes the principles of free access (which guarantees data subjects easy and free consultation regarding the form and duration of the data processing, as well as the completeness of their personal data), and non-discrimination (which prevents controllers of carrying out the data processing for illicit or abusive discriminatory purposes).

7.1.2 Art. 14, LGPD

511. The LGPD dedicates art. 14 to the processing of children's and adolescent's data. This provision is broader than art. 8, GDPR, and encompasses more rules than the ones relating to consent. Art. 14 states that children and adolescents' data must be processed in their best interests, pursuant to this article and specific legislation. The initial concern arising from the examination of this provision lies in the differentiation between children and adolescents. As a signatory to the CRC, Brazil should adopt a broad interpretation wherein the term "children" encompasses all individuals under the age of eighteen. However, the Child's and Adolescent's Statute (*Estatuto da Criança e do Adolescente* – ECA), which came into force in July 1990 and elaborates on art. 227, CRFB defines a child as an individual under the age of 12 and an adolescent as someone between the ages of 12 and 17.

512. Given the widespread use and recognition of the ECA's terminology, particularly within the legal field, the LGPD legislator decided to emphasize that data concerning adolescents should also be processed in accordance with their best interests. This differentiation becomes particularly pertinent when interpreting the paragraphs of this article, which establish specific rules for situations in which the data subject falls under the definition of a child according to the ECA, as elaborated below.

513. The CRC as a whole must be considered when interpreting any provision that affects the rights of children. However, emphasizing the importance of applying the principle of the best interests reinforces its critical role as a filter in any processing of personal data involving children and adolescents. While the article may not address all the issues arising from the

processing of their data in the digital environment, the inclusion of this principle directly in the provision has the potential to enhance the effectiveness of all the fundamental rights of this group (Henriques, 2023, p. 255).

514. Finally, the heading also mentions that processing children's data according to their best interest should take into consideration the other rules within its paragraphs, as well as in relevant legislation. This will certainly include any pertinent provision within the Brazilian legal system that may, in some way, affect this data processing. More specifically, this mainly includes the CRFB, the ECA, the CC and the CDC.

515. More specifically, the right to privacy is also recognized by art. 17, ECA, which provides that the right to respect consists of the inviolability of the physical, psychological, and moral integrity of the child or adolescent, including the preservation of image, identity, autonomy, values, ideas and beliefs, personal space and personal objects.

7.1.2.1 Children's consent and applicable legal bases for processing children's data

516. Art 14, §1º, LGPD states that children's data must be processed based on specific and explicit consent given by at least one of the parents or the legal representative. This rule should also be interpreted according to the broader Brazilian legal system.

517. The Brazilian CC presents two tiers of legal capacity. The so-called capacity of right can be considered a consequence of personality inherent to the condition of being a person (Menezes; Rodrigues; Bodin de Moraes, 2021). On the other hand, the capacity to act is linked to the ability to validly exercise civil life acts by oneself without the need for a representative or the consent of an assistant (Pereira; Lara; Rodrigues, 2023). The core of the capacity to act lies in the concept of discernment, through which capacity is measured by the efficiency of the outcomes of a person's choices (Menezes; Rodrigues; Bodin de Moraes, 2021).

518. Art. 3º, CC, defines individuals under 16 as absolutely incapable, which means that their will is disregarded by the legal system, and representation is necessary. On the other hand, art. 4º, CC, defines individuals aged 16 and 17 as relatively incapable. This means that these individuals can perform some acts directly, while they will need assistance for others (the incapable person participates in the civil life act jointly with their assistant). The child's representative or assistant are their parents (art. 1,690, CC) and in their absence a guardian appointed by a judge (art. 1,728, CC). Despite the recognition of the evolving capacities of the

child by the CRC, a static model purely based on age prevails in the Brazilian system as in many others around the world.

519. Over time, several other provisions have sought to mitigate the CC's rigidity, presenting exceptions to the general regime of civil incapacity, especially when personality rights are involved²¹ (Teffé; Fernandes, 2022). As presented above, the LGPD uses the ECA terminology of children and adolescents and not that of the CC. This led some legal scholars to argue that the LGPD should be interpreted in light of the CC, and parents' consent should be sought for processing data of every person under 16 (Gomes & Zappelini, 2020; Henriques *et al.*, 2020). However, considering that the LGPD is subsequent to the CC and the existence of other exceptions in the Brazilian legal system, it is possible to argue that the legislator has indeed introduced a new exception via *lex specialis*, allowing individuals aged 12 and older to consent to the processing of their personal data without representation or assistance (Densa, 2023; Fernandes; Medon, 2021; Teffé, 2020).

520. Just as consent given for the processing of sensitive data, the consent for processing children's data referred to in art. 14, §1º, LGPD, must not only have the same characteristics as the consent given for common data within LGPD (being freely given, informed, and unambiguous) but also be specific and explicit. Although the legislator has allowed adolescents to consent without parental representation or assistance, these two extra safeguards do not appear to be applicable to them.

521. Just as art. 8(2), GDPR, art. 14, §5º, LGPD, demands that the controller make all reasonable efforts to verify that consent had been given by the child's parents or legal guardian, considering the available technology. Here, two challenges arise, namely, what is considered reasonable efforts and what constitutes the available technology. Both challenges could be addressed through a case-by-case risk approach. The level of effort and technology used should be balanced with the processing of data that requires consent as a legal basis and with the best interests of the child as a whole, analyzing its necessity and proportionality. For example, if only the name and email of a child are going to be processed, it is not proportionate to use facial recognition technologies to verify consent, as this would entail much greater risk than the

²¹ For example, art. 1,740, III, of the CC, determines that it is the guardian's responsibility to fulfil other duties that normally fall to parents, after hearing the opinion of the child, if the child is already twelve years old or older; and art. 28, II, of the ECA, which determines the need for consent for adoption for people over twelve years old.

original processing activity. On the other hand, if the original activity is related to a child's health, for example, the threshold for verification should be higher.

522. It is important to mention that the provision of art. 14, §1º, has also raised several questions in relation to the legal bases applicable to the processing of children's data. Since it states that children's data must be processed based on specific and explicit consent given by at least one of the parents or legal guardians, many scholars would interpretate it as if consent was the only possible legal basis to process children's data.

523. This interpretation would be problematic for two main reasons. First, because art. 14, §3º, itself, as will be described below, provides two other legal bases for processing children's data for specific situations when consent could not be obtained. Second, this interpretation would not cover factual situations in which the best interest of the child needs to be enforced and where consent would not be applicable, such as in cases of legal obligation or when vital interests are at stake. Therefore, by using the best interest as an interpretative principle, it must be considered that other legal bases included in arts. 7º and 11 of the LGPD can and should be used (Fernandes, 2020).

524. In a preliminary study focused on the topic, the ANPD (2022a) also recognized many hurdles to implement a stricter interpretation. The DPA pointed out the illusion of control when consent is used in many cases; the excessive burden placed on parents or legal guardians; the impossibility of free consent in some instances (such as when there is a legal obligation to process data, as in education); the obstacle that it could create for children to have access to digital participation; the fact that parents are not always aware of all the risks for data processing; and the concern that it could be seen as creating a hierarchy between legal bases.

525. Art. 14, §3º stipulates that children's data can be collected without consent, when necessary to contact their parents or legal guardian (used only once and without storage) or for their protection. In neither of these two cases can the collected data be shared with a third party without parental consent. Thus, it is evident that these two specific legal grounds for processing children's data are reserved for highly specific and exceptional situations.

526. There is still no adequate and official understanding of what would constitute the protection of the child and the limits of the use of this legal basis. One possible way to interpret this basis would be to understand it in terms of "comprehensive protection", which is the object and scope of the ECA (art. 1). Considering that the ECA is the consolidation and elaboration of art. 227, CRFB, comprehensive protection could be understood as the duty of the Brazilian

State, the family, and society to promote all the rights of children and adolescents with absolute priority.

527. However, this interpretation would overly broaden the scope of art. 14, §3º, and this does not seem to have been the legislator's intention. It is possible to argue that the rule was formulated within a narrative of exceptionality. This becomes evident when considering that data to contact parents should only be used once and without storage or when, in both cases, data cannot be shared with third parties until consent is obtained (i.e. when the exceptional situation is remedied). Therefore, it is crucial to interpret this legal basis within the context of an extraordinary situation, encompassing protection against more immediate threats to the child's life and health.

528. Beyond the more restrictive interpretation of art. 14, §1º, as described above, another group of scholars argued that data concerning children and adolescents should be considered sensitive (Henriques *et al.*, 2020; Requião & Mendonça, 2023). It is important to highlight that, under the LGPD, sensitive data enjoy a special regime and a specific set of legal bases outlined in art. 11, which are different from the legal bases for the processing of general data found in art. 7º, LGPD. Unlike the GDPR, the bases provided in art. 11, LGPD are used on their own, without the need to combine them with a basis for processing common data.

529. Understanding children's and adolescents' data as sensitive data has the inherent advantage of automatically recognizing a stricter regime for the processing of this kind of data. However, Fernandes and Medon (2021) argue for the necessity of first considering whether all data concerning children can indeed be classified as sensitive before assessing the consequences of recognizing them as such and, more importantly, whether such classification is necessary.

530. First, the list of sensitive data includes specific categories of data and not of data subjects. In this regard, sensitive data includes, for example, those concerning racial or ethnic origin, religious beliefs, political opinions, etc., as per art. 5, II, LGPD. Therefore, the authors raise the question whether allowing children's vulnerability to justify treating all their data as sensitive, would not create the necessity of extending this understanding to the data of the elderly people and people with disabilities, for instance.

531. Secondly, the classification of data as sensitive is also tied to its potential for discrimination. However, a proper interpretation of the best interests principle has the potential to protect children's data much more broadly, as it demands comprehensive protection of children's rights, not solely limited to non-discrimination (Fernandes; Medon, 2021).

532. Lastly, this interpretation would hinder the possibility of creating an extra layer of protection for children's data that falls into the original classification of sensitive data, which could probably be considered "hypersensitive" (Fernandes; Medon, 2021; Teffé, 2021). In this regard, it seems evident that data concerning the religion, sexual orientation, and biometrics of these individuals, for example, should be protected even more rigorously than the same data concerning adults. Revisiting Luna's (2009) theory, we could identify two different layers of vulnerability, the one related to age and the one related to the processing of personal data which is potentially discriminatory.

533. Based on the issues described above, Fernandes and Medon (2021) suggest using children's best interests as an interpretative filter that should be applied *a priori* to determine which legal basis is appropriate to process children's data. In this regard, two legal bases could be seen as problematic: legitimate interest and credit protection (which will be further explained below). These are highly flexible legal grounds that may jeopardize, for example, the necessary transparency in assessing the best interest in each case. When it comes to legitimate interest, there is a need to balance rights in the specific case, which is done by the data controller. It would be the responsibility of the ANPD or the judiciary to conduct a *post hoc* analysis of the suitability of this legal basis, which increases the risk of violating children's fundamental rights. Regarding the legal basis for credit protection, it is evident that its purpose is strictly to protect financial interests, which may not align with the best interests of children.

534. This interpretation was adopted by two amendments to MP No. 1124/2022, which suggested transforming the ANPD into a special autonomous agency and initiated the process of independence for the authority (Mendonça; Rielli, 2022). The amendments were not included in the final text of the MP, and the situation was solved through an official interpretative statement by the ANPD.

535. In September 2022, the ANPD called for a public consultation regarding the possible legal grounds for the processing of children's data. In order to stimulate the discussion, the ANPD released a preliminary study (ANPD, 2022a), as previously mentioned, in which it recognizes three possible interpretations, disregarding the last one described above: (a) the application of consent as the only legal basis for processing children's data; (b) the application of the legal bases outlined in art. 11 to children's data; and (c) the possibility of applying all existing legal bases in the LGPD, as provided in arts. 7º and 11, depending on the data category.

536. In the study itself, the ANPD expressed a preference for the last hypothesis. This understanding remained unchanged even after several opposing positions from civil society and was released as an official Statement²². The same understanding was published in another Statement stemming from the IX Civil Law Conference²³, recognizing that art. 14 of the LGPD does not exclude the application of other legal bases, when applicable, as long as they observe children's best interests.

537. In the study, the ANPD highlights that even when more flexible legal bases are permitted to process children's data, they should be used with an additional layer of caution, considering children's vulnerability and the risks to their fundamental rights (ANPD, 2022a, parag. 64). This interpretation does not prevent the ANPD from establishing restrictions in the future related to the processing of children's data in specific situations, including with regard to the use of certain legal bases (ANPD, 2022a, parag. 73).

538. This was the case of the legal basis of legitimate interest, whose use was interpreted more restrictively by the authority in a specific guideline. According to the ANPD, legitimate interest should be used as a legal basis in a residual manner for the processing of data concerning children and adolescents in cases where there is: (i) a prior and direct relationship between the data subject and the controller, (ii) the processing aims to ensure the protection of the rights and interests of the involved child(ren) and/or adolescent(s), and (iii) when data processing is necessary to enable the provision of services that benefit the data subject (ANPD, 2024b).

7.1.2.2 Transparency obligations

539. Art. 14, §2º and §6º define specific transparency rules applicable to the processing of children's data. Art. 14, §2º states that when processing data related to art. 14, §1º, i.e., children's data processed based on parental consent, information about the types of data that are collected, how they are processed, and how the data subject rights in art. 18 can be exercised should be made public.

²² A Statement (Enunciado, in Portuguese) is a type of deliberative instrument with the purpose of interpreting the LGPD, which has binding effects on the ANPD. The aim of issuing a Statement is to promote legal certainty in relation to controversial issues (ANPD, 2023).

²³ The Civil Law Conferences are legal conferences held by the Brazilian Federal Judiciary with the aim of fostering debates among judges, scholars, and legal experts on unresolved issues in civil law and consolidating key doctrines through the formulation of statements that represent the majority of the members of each of the various committees (Aguilar Júnior, 2012; Conselho da Justiça Federal, [s. d.]). Although the statements are not binding, they are widely used as a reference by Brazilian authorities and the judiciary.

540. On the other hand, while the other paragraphs of art. 14 refer directly to art. 14, §1°, focusing on children as defined by the ECA, art. 14, §6°, applies to both children and adolescents since it refers to information about data processing mentioned in this article as a whole (which includes art. 14's heading on processing data in the best interest of children and adolescents). The information must be provided in a simple, clear, and accessible manner, taking into account the physical, motor, perceptual, sensorial, intellectual, and mental characteristics of the user. When appropriate, audiovisual resources should be used to ensure that the information is understandable for both parents or legal guardians and children.

541. This rule is of utmost importance within the context of the LGPD. Unlike the GDPR, the LGPD does not have a specific provision addressing transparency rules and mandatory information to be provided to data subjects. Art. 6°, VI establishes the principle of transparency, defining it as the guarantee of providing clear, accurate, and easily accessible information to data subjects about the data processing process and the controllers and processors of the data processing activity while respecting trade and industrial secrets. Therefore, art. 14, §6°, goes further and requires that the information provided about data processing be not only clear and accessible but also simple. Additionally, the controller must take into consideration the evolving capacities of the child and use other resources, such as audiovisual aids, to provide the information. This is especially important not only for children, as even when their parents or legal guardians consent on their behalf they are still considered the rights holders. It is also important for adolescents who may consent on their own according to the law and need information appropriate to their level of understanding and discernment.

7.1.2.3 Purpose limitation and data minimization requirements

542. Art. 14, §3°, stipulates that controllers are prohibited from making the participation of data subjects, as defined in art. 14, §1° (i.e., children according to the ECA), in games, internet applications, or other activities contingent upon the provision of personal information beyond what is strictly required for the activity. Its main objective is to discourage the “all or nothing” policies, where the user must either accept all the ToS or cannot use the application, which is common in standard form contracts (Teffé, 2020).

543. As previously mentioned, the LGPD includes in its art. 6°, III, the principle of necessity (i.e., data minimization), which, as defined by the law, entails restricting data processing to the minimum necessary, relevant, proportionate, and not excessive data required to achieve the

specified purposes. However, beyond reinforcing this principle, it is possible to argue that art. 14, §3º goes even further by using the expression “strictly necessary for the activity.”

544. Therefore, merely mentioning other purposes in the ToS is not sufficient to collect data beyond the main purposes of the application. Indeed, the LGPD determines that the principle of necessity is closely linked to the principle of purpose limitation: as long as it is a legitimate purpose, it is sufficient to announce it transparently, find an appropriate legal basis, and process the necessary data for it. In the case of children, however, it is necessary to refrain from purposes unrelated to the basic functioning of the application (Fernandes; Medon, 2021).

545. As an example of the practical application of this rule, consider that for a child to create an account in a particular application, only the essential information for the running of the game should be required. In other words, data collection should be reserved for enabling gaming, and it would not be possible to process data, for instance, for targeting advertising (Fernandes; Medon, 2021). Similarly, edtech should not be used to economically exploit children’s data for advertisement and for obtaining insights into children’s economic behavior. Therefore, the personal data collected must strictly adhere to (i) what is indispensable and (ii) what is justifiable (Zanatta; Valente; Mendonça, 2021).

546. This is an extremely important rule within the scope of the LGPD, which protects children’s data from the moment of collection and prevents them from being collected on a large scale for purposes unrelated to the main aim of the application or game in which the child is involved.

7.1.3 Other legal bases for processing children’s data

547. To process common data, the LGPD provides 10 legal bases in its art. 7º, which is four more than the GDPR. It can be said that the legal bases of consent, performance of a contract, protection of vital interests, compliance with a legal obligation, and legitimate interest are essentially the same in both laws. The legal bases unique to the LGPD are: Conducting studies by a research body, ensuring, whenever possible, the anonymization of personal data; the regular exercise of rights in judicial, administrative, or arbitral proceedings; protection of health, in a procedure conducted by health professionals or health entities; and when necessary for “credit protection,” such as in credit analyzes.

548. Furthermore, there is also a difference concerning the legal basis that can be used by public bodies. While the GDPR’s legal basis is broader and includes the performance of a task

carried out in the public interest or in the exercise of official authority vested in the controller, art. 7° of the LGPD only includes processing carried out by the public administration for the execution of public policies provided for in laws and regulations or supported by contracts, agreements, or similar instruments. In a significant ruling in Brazil, the STF decided that the execution of public policies was the only permissible legal basis from art. 7° and 11 that could be used for the purpose of sharing data by the public administration. The court understood that specific provisions in Chapter IV of the LGPD would provide additional legal bases for the processing of personal data by the public sector. For instance, art. 23 of the LGPD would allow the processing of personal data for the execution of legal competences or attributions of public services.

549. However, a recent guideline published by the ANPD on data processing by the public sector establishes that any of the legal bases defined in the LGPD, whether in art. 7° or art. 11, can be used by the public sector. When it comes to consent and legitimate interest, the examples provided are related to activities that have no direct correlation with public functions. Beyond the legal basis of executing public policies, the ANPD has determined that the fulfilment of a legal or regulatory obligation is a relevant and applicable legal basis for data processing by public authorities.

550. As previously mentioned, unlike the GDPR, the LGPD does not mandate controllers to find a legal basis in art. 7 and art. 11 for processing sensitive data. Instead, the legal bases outlined in art. 11 are considered sufficient on their own. Besides some minor textual discrepancies, the one present only in the LGPD is to ensure the prevention of fraud and to promote the security of the data subject in the processes of identification and authentication of registration in electronic systems (art. 11, II, g). In the case of the GDPR, it also provides some legal bases that are not present in the LGPD, namely when processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body (art. 9(2)(d), GDPR); and where the processing relates to personal data which are manifestly made public by the data subject (art. 9(2)(e), GDPR).

551. When it comes to schools, the same general guidance in relation to which legal basis could be employed under the GDPR is also applicable to the LGPD. However, two specific issues must be highlighted. First, during the public discussions regarding the LGPD, there was great pressure for consent to be waived in cases related to credit risk analysis. Intense lobbying led to the inclusion of a specific legal basis for credit protection. The authorization brought by

this legal basis is extremely broad and does not require specific safeguards, as is the case with legitimate interest, for example.

552. There is no precedent for this in other data protection legislation worldwide, and the ANPD has not yet issued any commentary on the topic. Consequently, there is no official guidance regarding the utilization of this legal basis for processing children's data. In its study on hypotheses for processing children and adolescents' data (ANPD, 2022a), the ANPD reinforced that, in its understanding, all the legal bases of art. 7 and 11 are possible to be used, but mentioned that there is a possibility that in future guidance, specific rules for the use of each basis will be defined. Thus, it is possible to use the best interests principle as an interpretative guide to preliminarily state that since the primary aim of this legal basis is to protect financial interests, it should not be used to process data from children and adolescents in Brazil.

553. Second, the LGPD also provides for another legal basis not included in the GDPR when it comes to sensitive data, namely the prevention of fraud and to promote the security of the data subject, in the processes of identification and authentication of registration in electronic systems (art. 11, II, g, LGPD). This legal basis could be used, for example, to process biometric data for authentication purposes in the use of edtech. Given the great sensitivity of these data, especially when it comes to children and adolescents, an in-depth analysis of necessity and proportionality needs to be carried out in each case.

7.1.4 Data subjects' rights

554. The data subjects' rights in the LGPD are fairly consistent with the ones in the GDPR. However, there are some differences and, in general, the LGPD provides fewer details regarding their exercise, considering that most of them are outlined in a single provision (art. 18).

555. For example, in relation to the right to erasure, this can be invoked when data are no longer necessary for a specific purpose, are excessive or non-compliant with the LGPD. Data processed based on the consent of the data subject must also be erased upon request, except in cases where the data are necessary for compliance with a legal obligation; for a study by a research agency, ensuring, whenever possible, the anonymization of personal data; transfer to a third party; or exclusive use by the controller, provided that the data are anonymized.

556. Another difference is encountered in the right to object to data processing. In the LGPD, a general right to oppose to the processing only applies when there is non-compliance with the law and there is no right to object to direct marketing.

557. Regarding the right to data portability, the LGPD merely states that it must be exercised according to guidance issued by the ANPD, which has not yet been published. The regulation of data portability in the LGPD does not restrict its scope to the data provided by the data subject, nor does it limit itself to specific legal grounds or the processing of data through automated means (Negri; Korkmaz; Fernandes, 2021).

558. Finally, it is important to mention that the LGPD does not grant data subjects a general right to object to solely automated decision-making. Art. 20, LGPD, only stipulates that data subjects have the right to request a review of decisions made solely based on automated processing of personal data that affect their interests. This includes decisions aimed at defining their personal, professional, consumer, and credit profiles, as well as aspects of their personality. It is worth noting the challenges brought about by the amendment of the LGPD by Law 13.853 of 2019, which removed the legal requirement that the review must be carried out by a natural person (Negri; Korkmaz, 2021).

7.1.5 DPIA

559. The DPIA is described in the LGPD as the documentation from the controller that contains the description of the data processing activities that could generate risks to civil liberties and fundamental rights, as well as measures, safeguards and mechanisms for risk mitigation (art. 5º, XVII, LGPD). While the GDPR specifies cases where a DPIA is required more clearly, the LGPD sets rules in a more scattered way.

560. The LGPD lists high-level situations in which the DPIA *may* be required by the ANPD, such as: in processing operations carried out for the exclusive purposes of public security, national defense, State security or investigation and prosecution of criminal offenses (art. 4, §3º); when the processing is based on the legal basis of legitimate interest (art. 10º, §3º); for public sector agents, including determination regarding the publication of the DPIA (art. 32); for processing involving sensitive data (art. 38).

561. While comprehensive guidance has not yet been issued, the ANPD specifies on its website that a DPIA must be conducted in any context where personal data processing operations may pose a high risk to the guarantee of the general principles of personal data protection outlined in the LGPD, as well as to civil liberties and fundamental rights of the data subject, in accordance with art. 5º, XVII, and art. 55-J, XIII, LGPD.

562. It also stipulates that controllers may, where appropriate, adopt as a parameter the concept of high-risk processing defined in art. 4° of the Application Regulation for small processing agents, approved by Resolution No. 2/2022 of the ANPD (2022b, 2023). This article includes the processing of data pertaining to children and adolescents as a scenario where high risk would be identified. This was also reaffirmed in a recent glossary developed by the authority (ANPD, 2024a).

563. In any case, assessing the impact of any decision on children's rights more broadly is already demanded by the principle of best interests itself. As already explained above, one of the aspects of this principle is its role as a rule of procedure, which demands that in any decision-making involving a child, a group of children or children in general, an assessment of its possible impact (positive or negative) on them should be carried out (Committee on the Rights of the Child, 2013a). In this sense, the evaluation must be used to explain how the best interests were considered in the decision, on what criteria it is based and how the best interests were weighed against other considerations (Fernandes; Medon, 2021).

7.2 The right to education

564. Art. 6, CRFB, guarantees the right to education, which is elaborated upon in arts. 205 *et seq.* According to arts. 205 and 206, CRFB education must be promoted and encouraged with the collaboration of society, aiming at the full development of the individual, their preparation for the exercise of citizenship, and their qualification for work. Its provision must follow basic principles such as equality of conditions for access to and permanence in school; freedom to learn, teach, research, and disseminate thought, art, and knowledge; pluralism of ideas and pedagogical concepts, and the coexistence of public and private educational institutions; the provision of free public education in official establishments; among others.

565. Primary education is free and compulsory for individuals aged four to seventeen. While the responsibilities for providing education are concurrent among the Union, states, and municipalities, the Constitution clearly defines the primary roles of each federative entity. The Union is tasked with organizing the federal and territorial education systems, funding federal public educational institutions, and serving a redistributive and supportive role through technical and financial assistance to the states, the Federal District, and the municipalities. The states and the Federal District oversee primary and secondary education, while municipalities

focus mainly on primary and early childhood education (as stipulated by art. 211, CFRB). The right to education is also guaranteed by ECA in its arts. 53 *et seq.*

566. The Guidelines and Bases of National Education (Lei de Diretrizes e Bases da Educação Nacional - LDB, 1996) is the primary legislative framework regulating both the public and private educational systems in Brazil, spanning from primary education to higher education. The law mandates that educational content, methodologies, and assessments must incorporate online activities to ensure that students grasp the scientific and technological principles underlying modern production (art. 35-A). Art. 80 also highlights the need to promote the development and dissemination of distance learning programs.

567. The Ministry of Education (*Ministério da Educação* - MEC) is the key Brazilian governmental agency responsible for formulating educational policies. At the federal level, the National Education Council (*Conselho Nacional de Educação* - CNE) contributes to the development of educational policies. Additionally, Brazil is committed to promoting the right to education under the UDHR (art. 26), the CRC (arts. 28 and 29), and the ICESCR (art. 13).

7.3 The Brazilian Artificial Intelligence Bill

568. Just like in the case of the AI Act in Europe, this section aims to simply outline the debate regarding AI regulation in Brazil. The discussion below will mainly focus on the content of bill 2,338/2023, which is still undergoing legislative proceedings in the Brazilian Congress and is still subject to modification.

569. AI governance has been under discussion in Brazil for some time now. In April 2021, the Brazilian Artificial Intelligence Strategy (*Estratégia Brasileira de Inteligência Artificial* - EBIA) was published by the Ministry of Science, Technology, and Innovation (*Ministério da Ciência, Tecnologia e Inovação* - MCTI), establishing nine thematic axes for the development of AI in the country. However, the document was considered by many as vague, not delving into essential topics such as planning and governance (Gaspar; Mendonça, 2021).

570. Regarding legislative initiatives, noteworthy are bills 5,051/2019, 21/2020, and 872/2021, which were filed in parallel with policy initiatives. In February 2022, the president of the Brazilian Federal Senate established a Committee of Jurists responsible for writing a draft bill on artificial intelligence in Brazil. After 240 days of work, which included hearings and public consultations, the final report with the draft was published, intending to replace the

three bills mentioned above. In May 2023, the draft bill was converted into a bill, the 2,338/2023 (Brasil, 2023c).

571. Bill 2,338/2023 reinforces the idea that there is not necessarily a trade-off between protecting fundamental rights and promoting innovation, seeking to align a risk-based with a rights-based approach. Apart from establishing rules for the development and deployment of AI systems in Brazil, it also encompasses rules for civil liability of AI systems.

572. In particular, art. 2° stands out for establishing the foundations on which AI should be developed and implemented, such as the centrality of the natural person, respect for human rights and democratic values, and the free development of personality. Art. 3° also enshrines basic principles, including self-determination, human participation, and non-discrimination. Chapter II contains various sections outlining the rights of individuals affected by AI systems, which apply horizontally to all cases. Of particular note is the extra attention accorded to vulnerable groups in art. 7°, §3°, which mandates that AI systems intended for their use must be developed in a manner that enables these individuals to comprehend their operations.

573. The bill also emphasizes the need to adapt the AI governance debate to the specific needs of the Brazilian reality (Bioni; Garrote; Guedes, 2023). The project acknowledges that asymmetries and structural inequalities permeate the country, and it includes, for example, definitions for direct and indirect discrimination derived from the Inter-American Convention against Racism. It also presents specific rules for the adoption of AI in the public sector, particularly in situations where individuals who are socioeconomically more vulnerable may be affected.

574. On the other hand, similarly to the AI Act, bill 2,338/2023 also contains specific rules that depend on the risk imposed by the AI system. This classification must be assessed by the AI system provider before placing it on the market or into service. Section II of Chapter III addresses AI systems that pose excessive risks and should be prohibited in the country. In comparison to the AI Act, the list is shorter, but the situations can be considered more comprehensive. In particular, emphasis is placed on the prohibition of the implementation and use of AI systems that exploit any vulnerabilities of specific groups of natural persons, such as children, in order to induce them to behave in a manner harmful to their health or safety, or contrary to the principles presented in art. 2° of the bill, including access to education (art. 2°, X).

575. Section III of the same Chapter addresses high-risk AI systems. Just like the AI Act Proposal, the Brazilian bill lists various categories of AI systems that may be considered high risk in its art. 17 and does not clearly define what can actually be regarded as high risk. Art. 18 determines that the competent authority can update this list based on a series of criteria, which include the impact on vulnerable groups. Within the list in art. 17, systems used for educational or professional training purposes stand out, including those that determine access to educational or professional training institutions or for assessing and monitoring students.

576. Art. 19 establishes governance structures and internal processes applicable to certain AI systems, such as transparency measures in the case of systems used in interaction with natural persons and for the mitigation of potential discriminatory biases. Apart from the requirements established in art. 19, high-risk AI systems must also comply with specific rules in arts. 20 and 22. They include conducting algorithmic impact assessments, keeping specific documentation, carrying out tests to assess reliability levels, establishing data management measures to mitigate and prevent discriminatory biases, and adopting technical measures to enable the explainability of the system's results.

7.4 Brazilian policy on digital education

577. The LDB states that distant learning can only be applied to primary education as a supplementary learning tool or in the case of an emergency (art. 32, §4º). With the COVID-19 pandemic, Law 14040/2020 (Brasil, 2020) was enacted to allow schools and higher education institutions to use online learning to meet the minimum workload required for their courses during the pandemic.

578. Regarding policies, the National Education Plan (*Plano Nacional de Educação* – PNE) was established by Law 13.005 in 2014, setting guidelines, goals, and strategies for educational policy from 2014 to 2024. Throughout the plan, several goals related to the implementation of ICT in education are mentioned, such as the development of pedagogical technologies that consider special education, rural schools, and indigenous and *quilombola* communities (Goals 2.6 and 5.4); the development and dissemination of educational technology, preferably open educational resources (Goals 5.3 and 7.12); and the promotion of full internet connectivity and access to computers in schools (Goals 7.20 and 7.22).

579. Goals 5.3 and 7.12 mention the need to give preference to free software and open education resources. In this vein, the MEC published Ordinance 451 (2018), which delineates

criteria and procedures for the production, evaluation, and distribution of open or free educational resources for primary and secondary education within official MEC programs and platforms. Art. 7º stipulates that educational resources created with financial support from the MEC for primary and secondary education must always be open educational resources.

580. It is also important to mention the Brazilian Strategy for Digital Transformation (Ministério da Ciência, 2018), which underlies the National System for Digital Transformation (*Sistema Nacional para a Transformação Digital*), established via Decree 9319, 2018 (Brasil, 2018a). This strategy extensively discusses open educational resources and highlights their potential to enhance access to quality education, thereby fostering innovative educational practices driven by digital culture (Amiel; Gonsales; Sebriam, 2018).

581. Also noteworthy is Commitment 6 of the 3rd Action Plan of the Open Government Partnership (2016-2018), co-created by the MEC and members of civil society, which aims to integrate the potential of digital culture into educational policy and to foster autonomy for use, reuse and adaptation of digital educational resources, valuing the plurality and diversity of Brazilian education (Ministério da Transparência, 2016).

582. Finally, in January 2023, the National Policy on Digital (Brasil, 2023b) was promulgated. The approach adopted by the policy is to coordinate programs, projects, and actions from different government levels to maximize the outcomes of related public policies. The PNED prioritizes actions aimed at the most vulnerable populations and is structured around four main pillars: digital inclusion; digital education in schools; digital training and specialization; and research and development (R&D) in ICT.

583. Regarding the digital inclusion pillar, the policy emphasizes various actions related to the development of digital skills, such as raising awareness, using tools for self-diagnosis of digital skills, training, developing platforms and repositories of resources, certifications, as well as the implementation and integration of connectivity infrastructure for educational purposes.

584. The pillar of digital education aims to integrate digital education into school environments, which encompasses acquiring knowledge about the digital world, computational thinking, digital culture, digital rights (including the protection of personal data), and assistive technology. In the pillar of Digital Training and Specialization, the twelve strategies are primarily geared towards higher education institutions and vocational education. The predominant aspect is the direct linkage of education to the demands of the workforce market.

585. Lastly, the R&D in ICT pillar aims to develop and promote accessible and inclusive ICT. This pillar lists six priority strategic actions, including fostering the development of low-cost ICT focused on education; promoting international partnerships; promoting open science and sharing digital resources among Scientific, Technological, and Innovation Institutions.

586. The LDB was also amended by the PNED to incorporate digital education and the provision of internet connectivity as part of the state's obligations concerning education in all public educational institutions (art. 4º, XII and sole paragraph).

587. The PNED will still be regulated by the federal Executive branch and does not have its own budgetary resources. It should be included in the multi-year national plan and in the budget laws in force until 2030 (Agência Senado, 2023). This means that the budgetary allocation for the PNED will have to compete with the already small portion of the education discretionary budget (the part not linked to mandatory expenses or programs whose funding sources are legally foreseen but allow for budget withholding or reallocation) (Seki; Venco, 2023).

588. Furthermore, the law also provides for state funds to finance actions related to the plan, such as the Telecommunications Services Universalization Fund (*Fundo de Universalização dos Serviços de Telecomunicações*), and the Fund for the Technological Development of Telecommunications (*Fundo para o Desenvolvimento Tecnológico das Telecomunicações*). Private entities will be able to enter into agreements with the public authorities for the implementation of the plan, in accordance with the regulation that will still be set by the executive branch (art. 11, sole paragraph).

589. The enactment of this law shows how the policy regarding digital education in Brazil has been shifting over the years, aligning with a more neoliberal approach. Several elements should be highlighted, such as the new state's spending cap, which reduces general public spending on education; the lack of inclusion in the law of specific budget for its implementation; its focus on promoting the use of "low-cost" digital technologies; and the encouragement of public-private partnerships. These elements demonstrate that a highly probable solution for the implementation of the plan regarding the digital technology infrastructure for education is the establishment of partnerships with foreign technology companies that offer their products for free or at a low cost due to their DDBM.

590. In the early 2010s, Brazil became internationally known for its strong engagement in the open educational resources community through laws and public policies that encouraged the use of licensed technologies in an open model in education and mandated public entities to

ensure that technologies developed with public funds were freely accessible (Amiel; Gonsales; Sebriam, 2018; Sebriam; Gonsales, 2017).

591. As will be discussed in the conclusion of this thesis, the focus on the development of open source technologies that consider local specificities is an interesting alternative to relying on big tech companies, which comes at a low cost but often at the expense of children's data protection. However, the coup d'état suffered in the country in 2016, the economic crisis, and the constant cuts in the education budget have made these policies increasingly hollow, which was further exacerbated by the COVID-19 pandemic. Without the necessary investment, it is more challenging to develop and procure sovereign technologies that are aligned with national interests and the best interests of children.

PART III. CHALLENGES INTRODUCED BY EDTECH TO CHILDREN'S RIGHTS TO PRIVACY AND TO THE PROTECTION OF PERSONAL DATA

592. This thesis asserts that, akin to all types of technology, it is imperative to maintain a critical and scientific perspective regarding both the opportunities edtech afford for humanity's advancement and the risks they entail. We have briefly seen in the introduction different ways in which edtech holds the potential to promote access to information, enhance accessibility—especially for children with disabilities—and optimize the efficacy and efficiency of learning. Nonetheless, apart from the absence of robust scientific evidence concerning the actual efficacy of the majority of current edtech in achieving their stated objectives, they may also be reinforcing problematic pedagogical practices (such as behaviorism and a learning-centric approach to education) and engendering adverse effects, such as the violation to children's rights to privacy and data protection.

593. Part III will use the research synthesized thus far to delineate the challenges introduced by edtech to these rights. Chapter 8 will concentrate on conducting a comprehensive mapping exercise of these challenges, divided into two main areas. The first part of the chapter will focus on horizontal challenges AI technologies pose, considering their prevalent role in contemporary edtech and data processing. The second part will delve into specific challenges introduced by three types of edtech included in the typology: personalized learning, student monitoring technologies, and learning analytics.

594. Chapters 9 through 11 will subsequently present a case study on the application of Google Workspace for Education in the EU and in Brazil to provide a concrete and more in-depth example of how children's fundamental rights can be at risk when using edtech. Chapter 9 focuses on understanding what Google Workspace for Education is, how it works, and what its role is within Google's business model. Chapter 10 discusses the implications of employing this technology to children's privacy and data protection in the EU and in Brazil. I will begin by analyzing decisions of authorities within the EU concerning this technology. This methodology was selected considering the audit and analysis capabilities of certain competent authorities, notably DPAs, allowing for a more in-depth understanding of the issues, which the mere assessment of ToS and Privacy Policies would not afford. This is also significant given the average data subject's inability to verify the validity of a company's claims within its policies.

595. Subsequently, I seek to understand the implementation of Google Workspace for Education in Brazil. The ANPD has not yet focused on the issues resulting from the application of this technology. Thus, in addition to a formal analysis of the ToS and Privacy Policies applicable to Google Workspace for Education in the country, secondary data obtained through a literature review were used for the assessment. This included research examining these documents in previous versions and also empirical research carried out via information requests to education secretariats in Brazil.

596. Finally, Chapter 11 undertakes a broader analysis drawing from the data collected in both jurisdictions to grasp the systematic operation of Google Workspace for Education through the lens of data colonialism. It also analyzes the extent to which the current data protection legal frameworks in the EU and in Brazil address these challenges.

Chapter 8. Mapping the challenges introduced by edtech

597. This chapter is dedicated to mapping the main challenges stemming from the use of data-driven edtech to children's rights to privacy and data protection. Considering that data processing predominantly occurs within AI systems nowadays, the first part of this chapter will concentrate on the overarching challenges presented by AI-powered edtech. Where possible, examples have been integrated into the text, supplemented by use cases in text boxes, to illustrate how these particular issues can be or have already been identified within edtech.

598. The second half of the chapter will focus on specific challenges related to three popular employed edtech, aligned with the typology developed in Chapter 1. We have discussed that technologies can be used for *providing education*—supporting educational institutions, teachers and learners—and for *learning about education*. Considering that many of the examples provided within the first part of the chapter pertain to technology that supports institutions (such as admissions or scholarship distribution algorithms), the second part of the chapter will focus on specific challenges brought about by personalized learning technologies (mainly focused on supporting students), student monitoring technologies (mainly focused on supporting teachers), and learning analytics (developed for learning about learning).

8.1 Datafication

599. As explained in Chapter 2, the measurement movement in education greatly benefited from the increased datafication enabled by digital ICT. Datafication can be understood as a way to put phenomena “in a quantified format so it can be tabulated and analyzed” (Mayer-Schönberger; Cukier, 2013, n.p.), which should not be conflated with digitalization—the process of converting analogue information into digital information. Data are “produced by abstracting the world into categories, measures and other representational forms—numbers, characters, symbols, images, sounds, electromagnetic waves, bits—that constitute the building blocks from which information and knowledge are created” (Kitchin, 2014, p. 1).

600. To capture something from the analogue world and transform it into digital data, it is necessary to measure and record it for analysis and value creation. Data are then often understood as the *representation* of a phenomenon², but it can also be “implied (e.g., through an absence rather than presence) or derived (e.g., data that are produced from other data, such

as percentage change over time calculated by comparing data from two time periods)” (Kitchin, 2014, p. 1).

601. With the increased possibility of dataifying new aspects of human life, the amount of data to be processed and evaluated by computers is enormous. Thus, the term big data started to be employed to refer to operations that “one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value [...]” (Mayer-Schönberger; Cukier, 2013, n.p.). AI systems, in particular analytics, started to be used to make sense of these big datasets, which would be impossible for humans.

602. The software model that is built on these data has three main characteristics: mapping (i.e., it is a projection, it is based on an original—reality); reduction (i.e. it reflects only a relevant selection of the original’s properties); and pragmatic (i.e. it is usable in place of the original for some purpose) (Kühne, 2005, p. 2). Indeed, a model is not a copy. Taking the development of a car as an example, if a copy is used in a crash test, a real test run would be performed, not a model simulation. Using a model has the advantage of being cheaper, but the drawback of often being inaccurate (Kühne, 2005, p. 3). If what is being datafied is human behavior and social relations, this copying exercise can be even considered impossible due to their complexity, instability and unpredictability.

8.1.1 Reduction and abstraction

603. Since datafication presumes measuring and quantifying complex phenomena of reality, it naturally captures only what is possible to measure with the current state of technology. It also entails reducing these phenomena into something that can be shared, analyzed and stored. The software model merely offers a limited representation of reality, and the decision regarding which data to collect for a specific purpose rests with the software engineers (Selwyn; Gašević, 2020, p. 530). The inevitable consequence is that these representations can fail to capture granular details from reality and important points of contrast.

604. What cannot or is hard to be directly measured, either because of a lack of technology or because it is too expensive or time-consuming, can be alternatively translated into usable data by proxies. A proxy is a variable or set of variables used as a substitute or approximation for a variable that a data scientist would like to measure. Proxies work through correlations, which will be better explained in section 8.2, *infra*.

605. Learning, for example, is hard to objectively measure because of its inherent complexity. It entails a multidimensional individual and collective process, involving, i.a., cognitive, affective, behavioral, and social factors. Several proxies could be used to evaluate learning, such as correct answers (and number of attempts to reach it) on exams, completion rates of lessons, participation in discussion fora, engagement metrics like click rates or time spent on a specific content, self and peer assessments etc. In a digital test situation, for instance, “rapid response times, alongside declining test performance may be associated with disengagement and guessing” (Wise, 2020, as cited in Maddox, 2023, p. 6).

606. The reduction of aspects of reality is closely related to the concept of abstraction, which refers to the process of removing information from its original context to be aggregated and processed (Pangrazio *et al.*, 2022, p. 262). This means that other information previously available in its original context that could help make sense of the data is removed or not even considered significant (Pangrazio *et al.*, 2022, p. 263). Again, which data are removed is related to the decision of which data are important for the model, which depends on the purpose of the collection and the pragmatic feature of software models discussed above. That means that using the data in other contexts is challenging and can lead to unintended consequences.

607. Removing the context from the collected data is inherently related to the idea that *what* is more important than *why* (using correlation instead of causation, as explained below). Therefore, datafying and modelling human life, especially within the school environment, has to be done very carefully and for very specific purposes. The purpose of the model directly influences the aspects of reality that are integrated and those that are excluded, making it very difficult to extrapolate this model to other situations. This creates a significant problem, for example, when the data production has as a final target its widespread sharing (such as in the development of “data products”), as there is a greater risk to misinterpreting the data in a different context.

608. Furthermore, we must consider the problem itself of quantifying education, as briefly discussed in Chapter 2. When it comes to education more broadly, certain aspects are simpler to quantify, such as learning content, leading edtech to prioritize these areas while overlooking crucial aspects that are not easy to measure, such as creativity, critical thinking, and social-emotional skills. This reduction of education to a mere compilation of skills and competences may result in decisions like narrowing the curriculum and favoring data sciences over humanities and the arts, given the greater difficulty in quantifying the latter (Holmes, 2023).

609. Within AI-driven edtech, students are also reduced to their digital twins, transformed into “calculable persons” who are assessed and evaluated based on their data (Lupton; Williamson, 2017, p. 787). Students are seen by AI systems as a model as well, which becomes a

make-believe substitution which can then be used to inform how the teacher approaches that student, or how an algorithmically personalized learning program assigns her tasks. As such, the substitute profile built out of the data takes an active ontological role in shaping the ‘real life’ of the student—a process that could always have been done otherwise, with different real world results. The data play a part in ‘making up’ the student (Williamson, 2019, p. 217).

8.1.2 Data collection for AI systems operation

610. The current operation of AI systems relies on the access to and utilization of a tremendous amount of data. Data are essential for training AI systems, and subsequently, it plays a crucial role in maintaining its relevance and facilitating adaptation for specific situations such as through profiling.

611. The massive collection of personal data in itself can be considered problematic not only due to the heightened risk of data breaches but also the potential for increased surveillance. As demonstrated earlier, when technology mediates all human behaviors and interactions, facilitating data recording, it enables various uses such as drawing inferences, creating profiles, conducting experiments, and influencing behavior for commercial and political ends (Sartor, 2020). In essence, what is fundamentally at stake (a focal point of the theory of data colonialism) is human and collective autonomy and flourishing. Having information about the entire society confers immense power upon the social quantification sector, which actually lacks democratic legitimacy.

612. Therefore, before discussing whether algorithms and datasets are fair, biased, or accurate, we should weigh the societal costs against the advantages of technology. We must deliberate on which systems merit development, who should oversee their creation, who holds the authority to determine their functions, what accountability mechanisms are necessary, and how individuals can participate in this process (Powles; Nissenbaum, 2018).

613. One example is data commodification and whether society deems data worthy of consideration as a tradable asset in the market, even in the absence of monetary exchange. This specific mindset surrounding of data, as we have seen in Chapter 3, creates market incentives to collect increasingly larger amounts of data and extend market’s influence into more and more aspects of human life. This is exacerbated when issues related to the market dominance of big

tech companies are discussed within a competition framework, as the solution often revolves around incentivizing data sharing and increasing the volume of data circulating in the market.

614. Apart from the massive collection of personal data in itself, we must also consider the challenges posed by the data sources used for training algorithms. When it comes to the data source, data may be collected explicitly for the purpose of training algorithms, repurposed if previously collected in other contexts, or scraped from publicly available sources on the internet. Each of these scenarios presents specific challenges, including ensuring compliance with the appropriate legal basis according to regulations such as GDPR or LGPD, meeting transparency obligations, ensuring compatibility for further data processing, and upholding data subjects' rights (Solove, 2024). Data scraping is particularly problematic, as even when the personal data being extracted is accessible in the public internet, it remains governed by data protection laws. It, therefore, raises concerns related to transparency and appropriate legal bases for processing data.

615. Finally, another important challenge relates to the tension between training AI systems and complying with key principles of data protection laws, such as purpose limitation and data minimization. These principles mean that only data necessary for specific purposes should be processed and this should be defined prior to the data collection. However, when data are collected for training AI systems, the exact purposes for processing them are often unforeseen by the AI developers. Considering that the GDPR and LGPD give more focus on establishing rules for the collection of personal data (which serves as input for the inferences made by AI) rather than on the outputs of this process (Wachter, Mittelstadt, 2017), it becomes difficult to perform meaningful purpose limitation or data minimization for data used to train AI systems, especially when dealing with general purpose AI (Wolff *et al.*, 2023).

8.2 Data Generation

616. A second challenge related to AI systems is related to how they produce knowledge based on the data they are fed with, and data analytics plays an important part in this process. *Analytics* is a field of computer science that uses ML techniques through mathematical and statistical algorithms to find meaningful patterns in data and, thus, insights. Davenport (2014) distinguishes three phases in the analytics history. The initial era of analytics 1.0 started in 1954 in the USA and was characterized by small, structured and internal data sources. At this time,

data was stored in large companies' warehouses or marts before analysis, and the analytical activity was mainly descriptive.

617. In the early 2000s, the exploitation of online data by companies such as Google, Yahoo! and eBay started the analytics 2.0 phase. Although in the beginning the analytical efforts were still mainly focused on internal and structured data, they started informing not only internal decisions but also customer-facing products and processes. Gradually, data began to be externally sourced, and the sets became either very large or unstructured, also being stored in parallel servers. That was the start of the so-called data-driven economy and the use of big data (Davenport, 2014).

618. Analytics 3.0 combines characteristics of the two previous eras. It is defined as the combination of “large and small volumes of data, internal and external sources, and structured and unstructured formats to yield new insights in predictive and prescriptive models” (Davenport, 2014).

619. Data analytics includes different technologies that can be clustered in many ways. It is not the intention of this thesis to present all the possible ways data analytics can be used and described, but some definitions are important for the discussions that will be carried out. Based on the outcomes of the analysis, for instance, data analytics algorithms could be descriptive, which means that they try to understand data from the past and provide solutions to influence the future. On the other hand, it can also be predictive, meaning that it tries to understand the present situation to predict the future.

620. Data analytics algorithms can also be clustered by their purpose. Educational analytics, for example, are understood as the use of analytics in education, which can serve different goals. If the goal is to optimize learning, this could be tackled by learning analytics, which is often defined as “the measurement, collection, analysis and reporting of data about learners and their contexts, for purposes of understanding and optimizing learning and the environments in which it occurs” (Siemens *et al.*, 2011, p. 4). The technical, ethical and pedagogical dimensions are explicitly integrated in this domain (Laet *et al.*, 2018).

621. Academic analytics, in turn, uses learners, academic and institutional data to improve organizational processes, resource allocation, workflows and institutional measurement (Siemens *et al.*, 2011). It focuses on strategic policy decisions and on how learning and educational results can be improved. It concerns, for example, figures on study success and drop-out rates (Laet *et al.*, 2018). More recently, the concept of student analytics has also

emerged, which primarily targets students themselves and study career counsellors. Its goal is to provide a personal and data-based student guidance by analyzing data factors for study behavior or success (Laet *et al.*, 2018).

622. Finally, educational data mining is yet another different technique for gaining insight into learners' activities. Unlike learning analytics, which “adopts a holistic framework seeking to understand systems in their full complexity [..., educational data mining] adopts a reductionistic viewpoint by analyzing individual components, seeking for new patterns in data and modifying respective algorithms” (Papamitsiou; Economides, 2014).

623. It is important to highlight, however, that there are no clear boundaries among these concepts. Institutional strategies directly affect learning, and learning results affect how institutions make decisions. Similarly, through a topic modelling of abstract data from articles on learning analytics and educational data mining, Lemay *et al.* (2021, p. 8) state that the difference between the two topics seem to be more a matter of degree than kind:

[b]oth fields were focused on student performance and learning platforms, and in modelling student behavior. [Learning analytics] papers focused more on student engagement, teaching tools, and social network analysis whereas [educational data mining] papers focused more on techniques and methods of data analysis.

624. As mentioned above, data analytics are used to recognize patterns or correlations among the data. After recognizing a pattern, the next step would be to extrapolate or deduce additional conclusions or predictions about causality based on the observed correlation. Therefore, this process does not adhere to classical scientific methodologies focused on identifying causation; instead, it relies on methods aimed at uncovering correlations.

625. “[A] correlation quantifies the statistical relationship between two data values. A strong correlation means that when one of the data values changes, the other is highly likely to change as well” (Mayer-Schönberger; Cukier, 2013, n.p.). With correlations there is never certainty, only probability. Statisticians will often choose a proxy and run a correlation analysis to discover how strong the proxy is. In order to first choose a proxy, they could use hypotheses based on theories, i.e., abstract ideas about how a phenomenon works. If they fail, the hypothesis or the theory it was based on needs to be revisited (Mayer-Schönberger; Cukier, 2013, n.p.).

626. It is also possible to use data mining, i.e. unsupervised/bottom-up data mining algorithms that are designed to identify relationships among data points without developing initial hypotheses. These algorithms do not rely on training data or predefined solutions (Hildebrandt, 2015, p. 24), and the patterns “discovered” by the algorithms can reveal

specificities of certain groups. This has important implications, especially for vulnerable people. An interesting example provided by Barocas and Selbst (2016, p. 691) in the context of employment can also be translated to the context of education. By providing more attention and opportunities to employees who are predicted to excel in a task, employers might unintentionally treat members of certain groups unfairly. This happens because the qualities that make employees attractive can be less common in these groups.

627. The focus on correlation instead of causation can also directly impact decisions made about students. For example, students who excel academically often allocate more time to the library or actively participate in the LMS. These behaviors can be associated with diligent studying, as high-achieving students typically engage in extensive preparation. However, encouraging other students to increase their LMS usage or time spent in the library, for instance, might not necessarily result in enhanced academic performance. Similarly, some of the outcomes generated by the data can be interpreted in different ways. If the algorithm identifies, for example, that students do not strictly adhere to the course schedule, with some studying ahead and others slightly behind the calendar, this can be understood at the same time as a problem or as an integral aspect of the adaptable and inclusive curriculum design (Weller, 2020, p. 145–146).

628. Understanding the reasons why some patterns exist is, in the case of big data analytics, often an afterthought. According to Mayer-Schönberger *et al.* (2013, n.p.), it is easy to get

caught in a web of competing causal hypotheses. But our attempts to illuminate things this way only make them cloudier. Correlations exist; we can show them mathematically. We can't easily do the same for causal links. So we would do well to hold off from trying to explain the reason behind the correlations: the why instead of the what. [...] [B]ig data itself aids causal inquiries as it guides experts toward likely causes to investigate [and i]n many cases, the deeper search for causality will take place after big data has done its work.

629. The instrumentalized “knowledge” generated by big data analytics can be seen, therefore, as representing a reversal of the values associated with the ideals of rationality and scientific inquiry (Kohl, 2021, p. 14). Subject matter expertise and domain-specific knowledge start to lose their significance, leading to a shift where computer and data scientists, rather than professionals like physicians, biologists, or sociologists, are increasingly seen as the primary protagonists (Rieder; Simon, 2017, p. 90).

630. It also directly affects the rights to privacy and to the protection of personal data by creating new data about people through inferences. These inferences, which include profiling and making predictions, often inform decisions that can directly impact people's fundamental

rights. The issues surrounding decision-making based on inferences will be explored further in subsection 8.3. However, it is first important to map the challenges related to generating new data itself, such as the presence of bias in the training data or design of the algorithmic code, as well as the lack of control of one's personal data.

8.2.1 Bias

631. Bias can manifest in various forms within AI systems, and given that data is sourced from society, where human bias abounds, it is difficult to think of a dataset without it. Data used to feed the system may be incorrect, partial or nonrepresentative, meaning that certain people or groups could be disadvantaged when decisions are based on these data (Barocas; Selbst, 2016). Prejudice could have played a role as valid examples to learn from, and the system will reproduce them.

632. Second, bias can also be imbued in the choices made by data scientists, either in the selection of the data that are included in the model, or in designing the algorithm code itself. The data that is left out of the analysis “is particularly problematic in educational datafication, since many of the issues that schools face have origins in structural inequalities that are not captured by, or considered in, data about student learning or teacher effectiveness” (Pangrazio *et al.*, 2022, p. 263).

633. Apart from defining which data to collect or not, the labelling process of the data by data miners or even users can also include bias in the system. Even when an AI model is “ready” it can continue learning with the user's behavior, which means that the prejudices and users' biased behaviors will also influence it (Barocas; Selbst, 2016, p. 682). In this sense, O'Neil (2016) argues that the choices made by data scientists are not just about logistics, profits, and efficiency but are fundamentally moral.

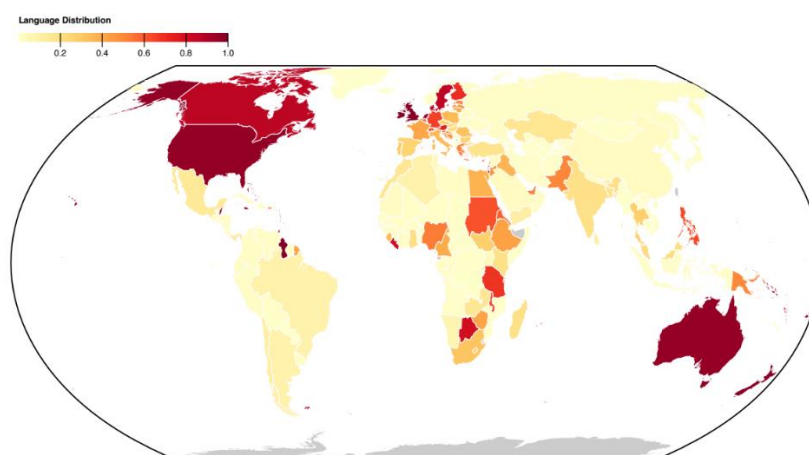
634. When it comes to the algorithm code, it can also be biased depending on how the data scientist designed it. For example, in a globalized world, edtech gets exported and used in contexts completely different from the ones where they have been developed. The constraints of a technology will be aligned with the ones of its designers, who are usually based on developed western countries (Pinkwart, 2016, as cited in Miao *et al.*, 2021). If the designers are a homogeneous group of people with the same background and worldview, this will often create bias and injustices, as they are less familiar with the educational necessities of other regions.

EdTech is neither ‘borderless, gender-blind, race-blind or class-blind’. The framing of the curriculum, as well as automated delivery in the mode that brooks no discussion,

marginalizes the knowledge of students—both indigenous and experiential—and reinforces existing epistemic injustices (Sarwar, 2022, n.p.).

635. One illustrative example is the dominance of the English language, which is frequently mandatory to participate in the digital environment. A recent research by Longpre *et al.* (2023) has developed a heatmap (reproduced below), which illustrates the extent to which the spoken languages of each country are reflected in the composition of natural language processing (NLP) datasets. It indicates that English-speaking and Western European nations are better represented when compared to other countries around the world.

Figure 4 - Global heatmap measuring how well each country's spoken languages are represented by the composition of natural language datasets



Source : Longpre *et al.* (2023, p. 12)

636. Within NLP, “coloniality can be connected to unstructured data, annotations, models and software. [...] In turn, these technologies reinforce and amplify coloniality beyond the social systems that created them” (Held *et al.*, 2023, p. 1–2). This limits and shapes a student’s experience, even when the content itself is translated, as language is intrinsically attached to a specific culture and epistemology. This dominance can also hinder digital literacy, an important factor for an efficient edtech (Sarwar, 2022, n.p.). Algorithms focused on personalized learning are also frequently biased towards “high income countries’ cultures and languages, which can result in a reinforcement of cultural hegemony and a suppression of local languages and cultures” (Holmes, 2023, p. 66).

637. Finally, it is important to mention that discrimination does not only occur when traits that are traditionally defined as potentially discriminatory are taken into account (such as data considered to be sensitive). Algorithms can also introduce new forms of discrimination that

were not previously anticipated (Solove, 2024). For instance, if an algorithm establishes a random correlation between a person's dominant hand and their academic performance, new types of discrimination may arise.

638. When it comes to edtech that aims to help educational institutions, one popular application is aiding in the student admissions process. In this context, an early and significant example of its adoption can shed light on the existence of bias in the training data, which is described in Table 2 below.

Table 2 - Franglen's Admissions Algorithm

639. From 1982 to 1986, St George's Hospital Medical School used a program to automate part of their admissions process. The algorithm was developed in the 1970s by St. George's vice dean Dr. Geoffrey Franglen, with the main motivation being to make the process more efficient and fairer because students would be subject to the same evaluation. After a double-test by human assessors and the program in 1979, the latter proved to be aligned with the panel's decision 90-95% of the time, and was put to use (McGregor, [s. d.]; Schwartz, 2019).

640. However, some lecturers recognized the lack of diversity among students and decided to conduct an internal review of the program. They concluded that irrelevant factors such as name and place of birth were being considered by the system, discriminating against women and people of color. The case was brought before the United Kingdom (UK) Commission for Racial Equality, which found the school guilty of discrimination. It identified that the biases already existed in the admissions process, with the algorithms merely learning from biased examples (Schwartz, 2019).

8.2.2 The challenge of controlling inferences based on personal data

641. As described in section 8.2, new knowledge generated by algorithms can take the shape of inferences, which, when made about people, can interfere in their rights to privacy and to the protection of personal data. Inferences can be drawn about basically any human attribute, state or behavior, including political opinion, emotional state, sexual orientation, shopping preferences, socioeconomic status, cultural background, dietary preferences, medical conditions, and location. Within the educational environment, inferences can be related to a

student's attention and engagement levels, academic performance and potential for success, learning disabilities, study habits, attendance patterns, personality traits, etc.

642. The operation of big data analytics presents a formidable challenge in discerning how data has been used to produce new information, directly affecting the control over one's personal data (Solow-Niederman, 2022, p. 361). This is tied to epistemic limitations of algorithms, i.e., constraints or shortcomings in the way they produce knowledge or "understand" a particular subject or phenomenon. Mittelstadt *et al.* (2016) propose three main epistemic limitations arising from the use of algorithms: i) inconclusive evidence, which underscores the probabilistic yet uncertain nature of knowledge derived from inferential statistics; ii) inscrutable evidence, which refers to the lack of clarity regarding how the different data points contributed to the generated conclusion; and iii) misguided evidence, which highlights the notion that the reliability of conclusions is contingent upon the quality of the input data.

643. From the individual's perspective, whether data was collected or produced by the algorithm is irrelevant; the ultimate outcome remains that new information about them has been produced that they might not have anticipated and might be used to make decisions that affect them. It can also uncover details that people do not intend to reveal or make wrong assumptions about them (Solove, 2024). Data is speaking on behalf of people, posing risks to the rights to their privacy, identity, development of personality, freedom of expression, reputation and self-determination.

These inferences, especially when people are not aware of them, persist over time and affect future opportunities and equal treatment (Mittelstadt, 2017), which can particularly affect children. The procedural approach of data protection laws have generally not been able to deal in a comprehensive way with these kind of challenges, as controllers are not obliged to disclose or justify the criteria and methods used to draw inferences. This led Wachter and Mittelstadt (2019) to argue, for instance, for a right to reasonable inferences as an accountability mechanism, which would offer additional protection against inferences that can cause reputational damage, violate privacy, or have low verifiability.

Table 3 - Inferring pupils' attention through brain waves

644. In 2019, some schools in China made headlines worldwide for implementing devices that monitored pupils' brainwaves. These headbands, provided by the company BrainCo, would sit across the students' forehead to infer their attention and was similar to devices used for detecting brain waves of patients in hospitals for medical assessments. They claim to be able to inform teachers and parents about how focused students are on their studies by detecting their brain signals—with different colored lights displaying the students' varying levels of concentration (Standaert, 2019).

645. While many parents and teachers see them as tools to improve grades, negative reactions from the public led the school to halt the experiment (Savillo, 2019). This case illustrates the expanding breadth of inferences that can be (allegedly) drawn from human beings, extending to the realm of human cognition.

8.3 Decision-making

646. After collecting the data, finding patterns, and creating new data, AI systems can be used to make automated decisions or aid in the human decision-making process. Automating decisions is often seen as a solution to streamline administrative tasks and help educators focus on more important issues, with the “bonus” of “remov[ing] politics and ideology from decisions” (Schildkamp; Kuin Lai, 2013, p. 2).

647. Nevertheless, students' lives can be profoundly impacted by decisions made based on data-driven technologies, particularly AI systems, potentially limiting their future opportunities (Jarke; Macgilchrist, 2021, p. 3). This section will concentrate on the primary challenges posed by the deployment of big data and AI systems to either automate decision-making or assist educators in making decisions regarding students. It will delve into specific types of inferences and the decisions based on them, such as profiling and future predictions, as well as scenarios where the human element directly intersects with the challenges posed by technology. Furthermore, it will address special situations where edtech is employed based on the typology adopted in Chapter 1.

8.3.1 Profiling

648. One way to infer data about people and make decisions based is to use profiling techniques. Algorithms use personal data and big data to analyze individuals' past preferences, behaviors, networks, and activities to create a profile of who they *were*. This information is used to infer their behavior, what may persuade them, such as a specific movie or advertisement, or their future actions and likes (inferences related to the future, i.e., predictions, will be dealt separately in the next subsection). As already explained above, profiling occurs when 1) a set of aspects about a person or group is inferred (a profile is created), and 2) the person or group is targeted based on these aspects (the profile is applied) (Bygrave, 2020a). Profiling raises concerns because of its very nature, as it involves “the pre-selection and pre-emption of individual choices by those who have access to big data sets and profiling technology” (Kohl, 2021, p. 5).

649. Although it may sound as if the individual is the focus, individual profiling involves classifying a person based on group attributes, which are used to place them into a specific micro-category (Kohl, 2021, p. 7). Cohen (2019, p. 69) argues that calling the process individualization is not entirely accurate. Individuals are probabilistically defined based on their past actions and undergo a process of rather singularization. Individuals are not adjusted to their unique characteristics by the profiler; instead, after providing some initial data, they are conformed to the profiler's standardized patterns (Kohl, 2021, p. 19).

650. In order to further unpack this process, it is first important to understand what “target variables” and “class labels” are within the data science language. Data analysis is a very broad that encompasses many different ways of understanding data. Simple forms of data analytics can produce records or summary statistics. Data mining, however, aims at locating statistical relationships, or patterns, in a dataset. “The accumulated set of discovered relationships is commonly called a ‘model,’ and these models can be employed to automate the process of classifying entities or activities of interest, estimating the value of unobserved variables, or predicting future outcomes” (Barocas; Selbst, 2016, p. 677). This is the process of finding correlations, as previously discussed. These qualities of interest are called *target variables* (i.e., what data miners are looking for), while the mutually exclusive categories that divide these outcomes are called *class labels* (Barocas; Selbst, 2016).

651. Translating a problem from reality to a question about the value of some target variable so that a computer can understand it is a very subjective process and it is possible to occur in a

way that disadvantages specific individuals or groups. When the categories the algorithm is looking into are not mostly uncontroversial (such as what is fraud or spam), they will always involve a value judgment (Barocas; Selbst, 2016).

652. Take, for example, the analysis of student excellence for admission to a university in a scenario where admission tests are not possible, as in the case of the COVID-19 pandemic. Calculating a student's grade can be carried out in several ways, such as through school records, curriculum, motivation, teacher recommendations, averages of similar students from the school they attended in previous years, evaluation of activities in the current year, etc. What is excellent, then, will be defined in ways that can be measured, but all of these options are just part of an almost infinite number of possible definitions of excellence.

653. The choice made can then have different impacts on different individuals or groups. In this sense, “[w]hile critics of data mining have tended to focus on inaccurate classifications (false positives and false negatives), as much—if not more—danger resides in the definition of the class label itself and the subsequent labeling of examples from which rules are inferred” (Barocas; Selbst, 2016, p. 680).

654. Therefore, the distinction between the individual and the group is likely to be misunderstood as they constantly and mutually influence each other: “[i]ndividual data feeds into population data sets and these sets produce, through correlations, knowledge about populations, that is patterns and groups within them (inductive), which in turn are instructive about the individual (deductive)” (Kohl, 2021, p. 8). The deductive process is related to distributive profiles (or universal generalizations), when the attributes are shared by all the members of the group (for example, in the category bachelor, all people share the fact that they are not married). On the other hand, non-distributive profiles “are framed in terms of probabilities and averages and medians, or significant deviances from other groups. They are based on comparisons of members of the group with each other and/or on comparisons of one particular group with other groups.” (Vedder, 1999, p. 277).

655. However, distributive profiles may also be understood in comparison with other groups when it comes to what they are *not* (e.g., the group *university staff* can be compared with *police* or *hospital staff*). This blurs the boundaries between the different types of profiles, and the certainty associated with distributive profiles becomes illusory (Kohl, 2021, p. 8). Ultimately, they can be considered as two different ways of looking at the same group or constructing groups.

656. When it comes to profiling and comparisons to group data, one frequent objection is the process of stereotyping, which occurs when people are evaluated or treated based on their membership in a particular group rather than recognizing their unique qualities and achievements as individuals. Take, for example, the use of academic credentials in hiring decisions. Employers

tend to assign enormous weight to the reputation of the college or university from which an applicant has graduated, even though such reputations may communicate very little about the applicant's job-related skills and competencies. If equally competent members of protected classes happen to graduate from these colleges or universities at disproportionately low rates, decisions that turn on the credentials conferred by these schools, rather than some set of more specific qualities that more accurately sort individuals, will incorrectly and systematically discount these individuals. Even if employers have a rational incentive to look beyond credentials and focus on criteria that allow for more precise and more accurate determinations, they may continue to favor credentials because they communicate pertinent information at no cost to the employer (Barocas; Selbst, 2016, p. 689).

657. This indirect profiling is opposed to direct profiling, which is based on data only about individuals themselves and is sometimes understood as a better way to profile individuals (Kohl, 2021, p. 10). However, arguing that direct profiling is more legitimate assumes that a person's past actions and preferences can accurately predict their future behavior and preferences. This perspective also implies that a person's identity is fixed over time. Direct profiling, like indirect profiling, is also inherently comparative and thus involves the social aspect of human life. Understanding individuality requires comparing it to a presumed "normality" that provides a context for individual differences (Kohl, 2021, p. 10–11).

658. Finally, even if the two processes are considered not so different from each other, there is still the discussion on stereotyping *per se* and its morality. Kohl (2021, p. 11) argues that stereotyping, or making non-universal generalizations, is a natural and necessary aspect of human knowledge and judgment, provided that it is based on empirical evidence and that certain historically disadvantaged groups are protected by anti-discrimination laws. This behavior, using shortcuts and proxies, is not inherently irrational or unethical and it is based on an acceptance of inaccurate results in particular cases (Kohl, 2021).

659. Hildebrandt (2008, p. 26) observes that to survive, all living beings must consistently analyze and profile their surroundings to adjust themselves or their environment. Therefore, big-data driven profiling and individualization can be criticized for *undue* stereotyping and for mistaking the reduction process for the totality of social knowledge (Pangrazio *et al.*, 2022, p. 262).

8.3.2 Predictions

660. Making predictions about the future is inherent to human nature. We do it all the time to mitigate the risk of uncertainty and the unexpected. With big data and the increase in data processing capacity, statistical techniques have become increasingly powerful and affordable. When it comes to predicting human behavior, what was initially more restricted to the finance sector (with the use of algorithms to predict whether a person would pay back a loan, for instance) has spread to all areas of life in society, including education.

661. Children are still evolving, and education itself is the implementation of human and economic resources betting on the development of individuals and society as a whole. Thus, predicting the future would facilitate anticipating challenges such as dropout rates, identifying areas for improvement, tailoring interventions regarding each child's educational path, resource allocation, etc.

662. However, unlike other types of algorithmic inferences, predictions are special because they involve the element of time, creating a unique set of problems. Decisions are made regardless of the prediction's accuracy and human rights violations can occur even when conclusions were right. As a projection of a possible future stemming from past or present perspectives, algorithmic predictions rely on certain assumptions that give rise to particular concerns. These assumptions are that i) the past repeats itself and the future will resemble it; ii) individuals will maintain consistent behaviors over time; and iii) groups with shared characteristics will share similar actions (Matsumi; Solove, 2023).

663. Matsumi and Solove (2023) cluster the problems arising from these assumptions and the use of algorithmic predictions based on personal data in categories. I will adapt them in this subsection while applying them to edtech.

8.3.2.1 Crystallization of the past

664. This issue is mainly based on the assumption that the past repeats itself. When algorithmic predictions are made about students based on past data about them, their families, their schools and their peers, it can perpetuate existing inequalities and limit their ability to explore and even think of alternative educational pathways and opportunities. These interventions can lock children into stereotypes, impede their social mobility, and influence their educational and other life opportunities.

665. Consider a student who is unable to attend classes due to her need to care for her ill mother. Hwe low attendance may influence predictions about this student's performance. However, if her mother's illness is cured, this aspect may not necessarily be factored into the decision-making process for her situation. Similar circumstances could arise when a student shows disruptive behavior at school due to family issues or bullying. Even if these underlying challenges are solved, decisions made solely based on a snapshot of a particular period in the child's life, rather than considering the entirety of their experiences and the potential for change, can lead to significant problems.

666. This is described by Williamson (2016, p. 137) as a "new form of 'up-close' and 'future-tense' educational governance", which transforms students into centers of anticipation. This kind of anticipatory governance "abducts subjects in specific habits; governs subjects through provided memories; and (dis)-orients subjects for calculable futures" (Webb; Sellar; Gulson, 2020, p. 2). This process is facilitated by data infrastructures that emphasize a linear, teleological, and quantifiable understanding of time, resulting in the synchronization of educational cultures.

667. Indeed, education policy has always been concerned with preparing individuals for an uncertain future and facilitating societal change. However, this form of anticipatory governance raises questions about whether future possibilities are truly knowable and how this could limit human agency. Rather than viewing educated individuals as having untapped potential waiting to be realized through education, they can be reduced to datafied subjects with predetermined paths. This approach restricts the range of possible educational futures, as they become mere continuations of past and present rearrangements (Webb; Sellar; Gulson, 2020).

668. This is especially problematic regarding children, as childhood is known to be a period of experimentation. Children test their limits all the time in order to get to know the world, inevitably making mistakes along the way. This does not mean that they will necessarily happen again in the future. On the contrary, we must recognize that most people change over time, particularly when they mature, and that it is unfair to view their past actions as determinants of future potentialities.

669. A study on errors of AI models predicting students at risk of not submitting their assignments can illustrate this. The researchers examined two categories of errors: false negatives, i.e., students who were anticipated to submit their assignments and did not, and false positives, i.e., students not expected to submit their assignments who yet did. The findings

underscored the importance of unforeseen events that can influence students' behavior and cannot be anticipated or accounted for in predictive algorithms, such as shifts in family and work obligations, unforeseen health concerns, and technical issues with computers (Hlosta *et al.*, 2022).

670. The dominance of chronological anticipations also obscures the ways in which the habits and memories of educated individuals are governed. In other words, the logic of time based on chronological order conceals how artificial intelligence determines future outcomes based on its own non-human algorithmic “learning”. The concept of aionic time²⁴, which encompasses different conceptions of time beyond the human perspective, is rarely discussed within education policy processes and practices (Webb; Sellar; Gulson, 2020).

671. Finally, when we zoom out from the individual to society, we realize that fossilizing the past necessarily maintains the status quo. The collected data tell a very specific narrative about the past, inherently limited to what was possible to gather and, more specifically, quantify. This leads to the oversight of underlying contexts and reasons, perpetuating existing inequalities.

8.3.2.2 Unfalsifiability and preemptive intervention

672. Two other very related problems described by Matsumi and Solove (2023) in relation to predictive algorithms are the impossibility of falsifiability and the problem of preemptive intervention. It is not possible to assert whether a prediction will ever occur in the future, meaning that individuals affected by decisions based on these predictions cannot effectively challenge them. Even though it is possible that the accuracy of the predictions can be determined in the future, decisions are often made before this time.

673. This creates another issue known as the preemptive intervention problem. Decisions based on the prediction interfere with the sequence of events in a particular narrative, making it impossible to know if the future event would have actually occurred or not. Consider an educational institution that implements a student retention program using algorithmic predictions. If a student's probability of dropping out in the next semester exceeds a certain threshold, the student will be enrolled in additional support programs. A student is at high risk of dropping out, so the institution provides them with extra academic and counseling support and they complete the semester]. In this scenario, it is impossible to know if the initial

²⁴ “Aionic conceptions of time stress the quality of duration (e.g., ‘eternal’, endless, cyclical) and differ from chronological conceptions of time that stress sequencing of events and binary teleologies that extend backwards or forwards (e.g., past and future)” (Webb; Sellar; Gulson, 2020, p. 6).

prediction was wrong or if the institution has just timely intervened in the situation. A narrative arguing that the algorithm prevents dropouts is thus challenging to refute.

674. This presents specific challenges regarding accountability and data control, akin to those discussed in section 8.2.2 above. However, these challenges are exacerbated due to the element of time and the inability of individuals to provide counterevidence to the prediction. When it comes to inferences about the present, it is easier to be verified (think of a person's political affiliation, for instance), but inferences about the future are always speculative (Matsumi; Solove, 2023).

8.3.2.3 Performativity

675. As discussed above, unsupervised algorithms use a bottom-up approach to identify relationships among data points and create clusters. This means they will try to find patterns among the data that were not previously thought of. The very nature of clustering algorithms introduces uncertainty regarding whether the generated groups accurately represent the data's underlying structure or if artificial groupings have been created. Different clustering algorithms with distinct properties can yield different results, and selecting a clustering criterion further influences the outcomes, as different criteria can impact the created groups (Perrotta; Williamson, 2018, p. 10).

676. This means that patterns are not just "found" by algorithms but actively constituted. The concept of "performativity" is relevant here, as it suggests that social practices, knowledge forms, objects, and analytical tools are not mere representations of reality but are involved in reproducing it (Perrotta; Williamson, 2018, p. 4). Selwyn (2015, p. 72) argue that using a digital data lens can lead to the idea that complex (and mostly unsolvable) social problems within schools can be seen as complex (but solvable) statistical problems. Therefore, data analysis starts to shape educational settings in the same way that educational settings produce data.

677. Floridi (2011, p. 30, emphasis in the original) explains that information can be understood in three ways: "information *as* reality (e.g. as patterns of physical signals, which are neither true nor false), also known as environmental information; information *about* reality (semantic information, alethically qualifiable); and information *for* reality (instructions, like genetic information, algorithms, orders, or recipes)". This means that information can deeply impact reality by changing the knowledge about it, constituting it, or changing it (Purtova; Maanen, 2023, p. 10). The extent of this impact depends on the intricate interplay of various

factors that underly the process of datafication and the use of algorithms, including interests, choices, and technical considerations.

678. Algorithmic predictions may crystallize a student’s perceived status and result in, for example, low expectations, which leads to a self-fulfilling prophecy of failure. This is known as the Pygmalion or Rosenthal effect, which refers to a psychological phenomenon where high expectations leads to improved performance. When certain behaviors are anticipated from others—due to any specific bias, be it good or bad—human actions tend to influence the likelihood of those expected behaviors occurring (Perera, 2023). The labels created to categorize students are internalized not only by them but also by their educators. This influences both behaviors towards what was initially expected and not necessarily to a child’s full potential.

679. Studies show, for example, that increasing the amount of a scholarship (or conversely, increasing the amount of debt) directly increased graduation rates. Additionally, scholarships can influence a student’s attitude and commitment towards college (Engler, 2021). This evidence suggests that using predictive algorithms, which rely on past data to award scholarships—a practice increasingly observed in universities—might overlook this effect and directly impact individuals’ likelihood of graduating.

680. The table below illustrates two similar cases highlighting the issues with predictive algorithms. It demonstrates how these algorithms, used to assess students, crystallized past situations; made it impossible for students to counterprove the results; and, if their use were not discontinued, they could potentially begin shaping reality, influencing how schools teach students or organize themselves to better align with the algorithm’s assessment criteria.

Table 4 - Ofqual’s algorithms for evaluating students’ performance

a) England

681. In England—with a similar situation taking place in Scotland (Scottish school pupils have results upgraded, 2020) —algorithms were used for evaluating students’ performance in secondary school. Due to the cancellation of all secondary education exams as a result of the COVID-19 pandemic, an alternative method had to be developed for assessing students’ achievements. The Office of Qualifications and Examinations Regulation (Ofqual) initially

requested that teachers predict their students' grades, but it was worried that they might be too optimistic. Therefore, an algorithm was also implemented to standardize grades.

682. The model was complex and encompassed various layers of assessment. According to Bedingfield (2020, n.p.), first, it created a historical profile of grades achieved by students in each subject at each school over the past three years. The algorithm then generated three sets of grades, comparing the distribution of grades from previous years to predict distributions for past and current students based on national averages for similar prior attainment.

683. The algorithm calculated the difference between the predicted distribution for current and previous students, adjusting the actual distribution of earlier students to give a distribution for current students. Grades were assigned based on a ranking provided by teachers. Even if a student was predicted a certain grade, they could still receive a lower one if the pupil ranked at the same level the year prior received a lower grade. While the percentage of "A" grades reached a record high of 27.9%, the algorithm reduced nearly 40% of the A-level grades forecasted by teachers. Many students failed to meet university entry requirements, and neither the International Baccalaureate Organization (IBO), which offered the algorithm, nor Ofqual have properly explained how the final grades were awarded (Cyndecka, 2020).

684. This model was problematic for various reasons, such as for penalizing excellent schools and students because of the national average; penalizing great students in underperforming schools; privileging independent, smaller and richer schools because cohorts that averaged smaller than five were given only their teacher's predictions; and lacking accuracy and transparency in its testing (Bedingfield, 2020, n.p. Dark, 2020). Digital rights' organization Foxglove threatened to take legal action against Ofqual on the bases that the algorithm was evaluating schools instead of students and this automated decision would violate art. 22 of the UK GDPR (Dark, 2020). In the end, students protested against the use of the algorithm and only the grades predicted by teachers were used. This does not mean that problems such as incorrectly estimating the performance of black students did not occur (Cowan; Arboine; Alemoru, 2020).

b) Norway

685. The same algorithm provided by IBO was used in Norway and was investigated by *Datatilsynet*, the Norwegian DPA. The DPA has received several inquiries related to reports issued by Norwegian media regarding students who believed their final grades were not accurate. According to the DPA's request for information letter sent to IBO in July 2020, some students believed that using historical prediction data from the schools would lead to being evaluated similarly to their peers of previous years, even when individual differences existed. Being this an automated decision-making process, it would be prohibited, unless exceptions of art. 22(2), GDPR, applied (*Datatilsynet – Norwegian Data Protection Authority, 2020c*).

686. In the following month, the DPA issued an advance notification of order to rectify unfairly processed and incorrect personal data to IBO. The DPA intended to decide that a) IBO refrained from using “school context” and “historical data” in awarding grades to students, as this would violate the fairness principle in art. 5(1)(a), GDPR, and lead to the processing of incorrect personal data in violation of art. 5(1)(d), GDPR; and that b) IBO rectified grades awarded under these criteria (*Datatilsynet – Norwegian Data Protection Authority, 2020a*). This action led to some students receiving higher grades. However, the DPA did not have the competence to challenge them further. The IBO's main office was in the UK, which was still part of the European Economic Area (EEA) at the time, meaning that the Norwegian DPA could not take further actions (*Holmes et al., 2022*).

8.3.3 Human mis-interpretation and mis-use of data

687. Human interpretation of data within the school environment can result in wrong and unfair decisions, creating new or perpetuating old inequalities. After misinterpreting the data and making incorrect assumptions, educators could focus on improving the wrong issues (*Lai; Schildkamp, 2013, p. 18*). If a student is performing poorly, for instance, educators may try to interpret the causes of their academic outcomes (*Bertrand; Marsh, 2015, p. 864*) (although, as already discussed, causation is not the approach to data taken by algorithms). Schools could, attribute students' performance solely to their categorization by an algorithm (such as identity, services received or test scores). They can assume inherent deficiencies (e.g. the student's outcome in English is not excellent because of its migration background) instead of reflecting on historical inequalities, their own instruction or considering how the school can better support these students. When educators use data ignoring their context or rely on personal assumptions

about students or their families, it can reinforce pre-existing biases and the unjust context that shapes student outcomes (Bertrand; March, 2021). It also prevents them from getting to the root of the problem and making the right decision to improve educational processes.

688. There is also the challenge of placing too much trust in technologies, often leading to overshadowing educators' reasoning and experience, even when evidence suggests otherwise. Research has shown, for example, that people tend to obey instructions from a robot in a simulated fire emergency, even when they are informed that the robot was malfunctioning and the guidance provided was evidently incorrect (Wagner; Borenstein; Howard, 2018). This means that educators will require training and assistance to comprehend how and when they must apply their own judgment (Cardona; Rodríguez; Ishmael, 2023, p. 32).

689. This is also linked to what is currently known as the dashboard effect. After the data are analyzed by a specific system, the information is often presented to educators through a dashboard or other type of visualization technique. This effect means that individuals or organizations make decisions solely or mostly based on the information presented in a dashboard or visual display of data without considering the broader context or additional information. It is easy to become overly reliant on the simplified and summarized information provided in a dashboard, potentially overlooking important details, nuances, or underlying complexities.

690. Even if people were to become aware of the context and all the information needed to interpret the data—which is very difficult due to algorithms' black-box feature (Laet *et al.*, 2020)—dashboards, as well as the data embedded on them, rather than being impartial representations of reality, are shown to construct compelling narratives. These narratives have the tendency to portray teachers as managers, students as varying degrees of risk, and reduce the complexity of students' social interactions to quantifiable data points (Jarke; Macgilchrist, 2021, p. 3).

691. The use of dashboards in edtech, as well as other kinds of data visualization, “makes data about children into a form of value that can be exchanged by them for rewards such as upgrades and personalized features, transforming classrooms into little digital economies and calculative spaces where personal data have exchange value and utility” (Lupton; Williamson, 2017, p. 787).

692. Dashboard views also “create a false sense of autonomous control over learning while nudging teachers' interpretations and pedagogical actions through particular views. [... They

are] always biased reductions of learning—and not in any way neutral representations [...]” (Kerssens; Dijck, 2022, p. 295). The increasing reliance on data-driven decision-making may affect educators’ pedagogical assessment and intuition, as their importance can rapidly be diminished compared to the digital devices that students are required to use (Hillman *et al.*, 2023).

693. This effect can certainly be identified both in descriptive and predictive analytics. Although research on predictive systems in education is limited, the existing ones indicate that teachers and other users can modify their behavior based on dashboard outputs. This raises ethical concerns, as exemplified by a user questioning whether they should advise students labelled as “high risk” to pursue alternative paths instead of college (Hartong & Förschler, 2019, as cited in Jarke; Macgilchrist, 2021, p. 3).

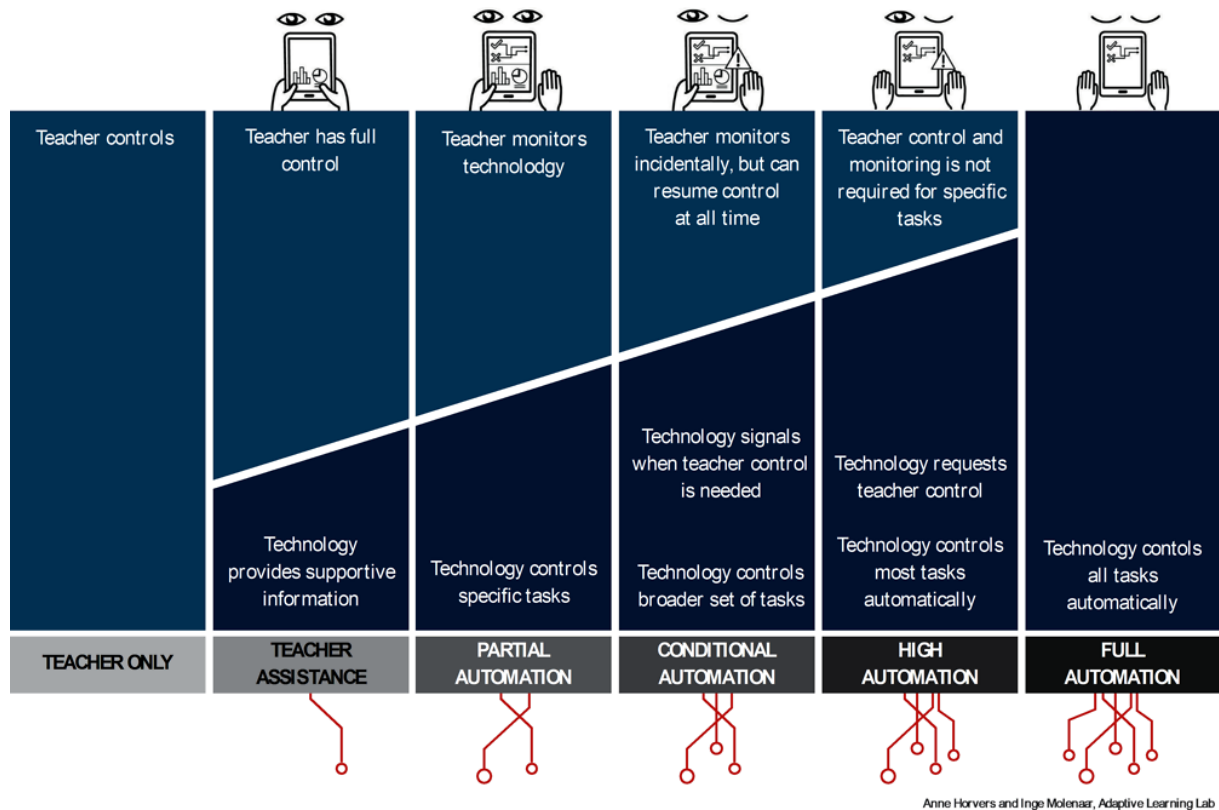
694. They can thus also play a role in undermining educator’s professional autonomy and expertise. Educating a child is highly nuanced and context-dependent, which requires flexible and adaptive approaches. Relying on predefined metrics and algorithms, especially when these are seen as more “objective”, can limit the ability of educators to make informed decisions that are also based on their knowledge, experience, and instinct (Zeide, 2020).

695. To understand the level of automation and teacher participation within personalized learning technologies—which could also be used here to discuss how edtech can impact educators’ autonomy—Molenaar (2021) suggests six levels of automation defined by the car industry to the field of education (see Figure 5 below). Here, we can clearly see how industry standards and epistemologies (as discussed in Chapter 2) are increasingly being applied to education.

696. According to the original model’s explanation (Molenaar, 2021, p. 59),

[t]he lines under the model represent the expectation that increasingly more data streams will be used in the transition towards full automation. These data streams can support more accurate detection and diagnosis of learners and their environment. At the top of the model, the level of human control is visualized across the levels. The hands on the tablet represent the level of teacher control. Full teacher control with two hands on the tablet, partial control with one hand and no hands symbolizes no or incidental teacher control. The eyes represent the required level of teacher-monitoring, ranging from full, partial, incidental to no monitoring. The warning triangle indicates the ability of the AI to notify the teacher to resume control at critical moments.

Figure 5 - Six levels of automation of personalized learning



Source: Molenaar (2021, p. 60)

697. These possibilities create several tensions around teacher's control. A scenario where the technology is in full control with no teacher involved would rarely be desirable, but the middle ground is full of nuances and gives rise to different challenges. We might need to establish guidelines that would vary on a risk-based approach. More caution should be taken when handing over control of critical decisions, such as determining a student's placement in their next course or managing disciplinary referrals (Cardona; Rodríguez; Ishmael, 2023, p. 31).

698. Similarly, these decisions may also require a very granular understanding of what it means to have humans in the loop or in control. This could include always requiring teachers' input establishing protocols for further intervention of principals, municipalities, or student associations where necessary, as well as granting students due process rights. However, it is also important to recognize that including teachers in the loop might also create more work than what they previously had, which mitigates the initial attempt to make their job easier (Cardona; Rodríguez; Ishmael, 2023).

699. Finally, another situation where data could be misused is by trying to “game the system” (Laet, 2023, p. 52). This would involve the attempt to be successful in the educational digital learning environment by exploiting its social-technical properties, instead of using it as a tool to achieve the previously defined educational goals.

700. Schools might manipulate student data to boost their own performance metrics; emphasize short-term achievements, compromising the long-term learning process; tailor the course content or focus only on some students in order to improve score tests at all costs (Lai; Schildkamp, 2013); focus on hacks to master standardize tests, etc.

8.3.4 Personalized learning

701. In a traditional classroom, students follow the same curriculum and perform the same tasks. Credits are generally awarded based on “seat-time”, regardless of what is actually learned, and the focus is on the development of the average student, not the full potential of each individual. Even in this traditional scenario, however, everyday interactions within the classroom already include some degree of personalization, such as when teachers provide extra support to students who are struggling to make progress, which requires educators to have a deep awareness of the needs of each student (Holmes *et al.*, 2018).

702. Personalized learning is thus not a straightforward concept. It can encompass a wide range of approaches and there is no universally accepted definition, with different educators and experts interpreting and implementing personalized learning in different ways. It is also often conflated with other concepts such as individualized learning, competency-based learning and differentiated learning, whose meaning will often depend on the one defining it.

703. Although complex and very much contextual, it is possible to map some common features of personalized learning from the existing understandings. According to Holmes *et al.* (2018, p. 16), these features would involve multiple continua related to micro and macro decisions taken by the network of actors within education. The more agency learners have in relation to designing their own learning process, the more personalized the learning process can be. These continua include:

Personalisation of why something is to be learned (the learning aims); Personalisation of how it is to be learned (the learning approach); Personalisation of what is to be learned (the learning content and learning pathway); Personalisation of when it is to be learned (the learning pace); Personalisation of who is involved in the learning (the learner or learning group); Personalisation of where the learning takes place (the learning context).

704. As we have seen above, the idea of personalized learning is not a new one and started to be discussed well before the development of existing technologies. It is at the core of progressive education traditions, which emphasize tapping into students' interests and passions, providing them with individualized opportunities to ask questions, explore, and take risks to facilitate learning. This approach is related to the work of the American educator John Dewey over a century ago, for instance, and is commonly found in schools that prioritize project-based learning (Herold, 2019, n.p.).

705. However, personalizing learning was also very important to behaviorist approaches at the beginning of the twentieth century. Behaviorism is a psychological theory that emphasizes the study of observable behaviors, rather than internal mental processes. According to behaviorists, behavior is shaped by environmental factors, such as rewards and punishments, and can be modified through conditioning techniques.

706. Human beings are understood as “organisms” that should be observed in order for psychologists' work to be considered scientific. The loss of the human inner world's importance (as it would be exempted from scientific inquiry) and the understanding that the environment determines human behavior have several consequences for autonomy and free will. What is viewed as outcomes of free will should be seen just as the accidents in the world of physics (Zuboff, 2019).

707. The behaviorist approaches to learning, for example, seek to reinforce desired behaviors and shape them through systematic instruction and practice. Mastering academic content could be fostered by identifying what each child needs to learn, assessing what they already know, and then creating an optimal path for them to learn the rest. As detailed in Chapter 1, the implementation of this approach can be traced back to the 1950s when the behaviorist B. F. Skinner experimented with “teaching machines”, which allowed students to answer questions and immediately receive feedback (Herold, 2019; Watters, 2021).

708. As can be expected, the problem with this theory is that it views personalized learning not only as rooted in a measuring and testing rationale but also as completely detached from the development and significance of students' autonomy. It fails to encourage self-knowledge, thereby hindering individuals to understand their capabilities and difficulties, as well as the best path towards integral human development. This approach merely identifies, through observable behavior (which can be embedded in biased interpretation and correlations), what the students

know and need to know, guiding the learning path from one point to another through behavioral steering techniques.

709. Understanding this history is important because technologies can reflect different understandings of learning and different pedagogical theories. Many argue that the way personalized learning is embedded in today's edtech is mostly based on behaviorist and instructionist knowledge-transmission approaches, rather than on educating by projects, collaborative learning, guided discovery learning or productive failure approaches (Miao *et al.*, 2021; Watters, 2021).

710. If the learning process is narrowly conceived as the transmission of pieces of information, that will eventually build into knowledge and skills, then automation would be a way to enhance the efficiency of this process. If the goal, however, is to enable children to understand concepts from within and encourage them to find answers to their own inquiries about the world, then their approach to learning is somehow already unique and diverse (Kohn, 2015).

8.3.4.1 Technologies for Personalized Learning

711. Although personalized learning can be perceived as an interesting and pedagogically sound approach, it is challenging to implement in traditional, large classrooms. It requires training, specific resources, time, and alignment with the educator's own approach. Ideally, it demands a democratic discussion on who decides what, and where a school lies within each of the personalized learning continua mentioned above.

712. Technologies are historically seen as an important tool to support personalization (see, for example, the development of teaching machines described in Chapter 1). With advanced tracking capabilities, it has become easier to monitor students' learning plans and progress with greater precision, while enabling a wider range of instructional opportunities (Pane, 2018, p. 3). Other developments such as the availability of one device per student in many countries and a deeper integration of technology into daily school practices have also played an important role (Molenaar, 2021).

713. Intelligent Tutoring Systems (ITS)—also known as intelligent interactive learning environments—, for example, “provide step-by-step tutorials, practice exercises, scaffolding mechanisms (e.g. recommendation, feedback, suggestions and prompts) and assessments, individualized for each learner, through topics in well-defined structured subjects such as

mathematics or physics” (Holmes *et al.*, 2022, p. 5). When the ITS is based on dialogues about the subject instead of an individualized sequence of material or activities, it is also called Dialogue-Based Tutoring System (DBTS).

714. ITS can come in many shapes and is sometimes implemented in LMS such as Moodle, Open edX and platforms like Khan Academy (Miao *et al.*, 2021). They mainly involve several AI models, such as a domain model (knowledge about the topic to be learned), a pedagogy model (knowledge about effective approaches to teaching) and a learner model (knowledge about the student). Some ITSs also involve a fourth model called open learner, which aims to provide information to teachers and learners on what has taken place within the system and the decisions made (Holmes; Bialik; Fadel, 2019, p. 102–107).

715. Making use of a learner model, i.e., a hypothesized knowledge state of a student, is actually what really differentiates AI-driven ITS. It incorporates thousands of data points from the user, such as which tasks they have answered correctly and what challenges them, what is clicked on the screen, what is typed, how rapidly they move the mouse, as well as their emotional state. Through data analysis, this is integrated with the knowledge about other students and their interactions to predict the suitable pedagogical approach and domain knowledge for a specific student at any stage of their learning (Holmes; Bialik; Fadel, 2019, p. 105). These data are also used to update the model, and the cycle starts again.

716. As mentioned in the definition of ITS, these systems are better suited for well-defined domains such as mathematics and physics. One reason for this is that imprecise problems would generally require students to apply other more complex skills and the contexts would be more dynamic and uncertain. The lack of structure challenges the definition of learning paths and the provision of feedback (Holmes; Bialik; Fadel, 2019, p. 108–109). An alternative to ITS is Exploratory Learning Environments, which adopt a constructivist approach. In these systems, students actively build their knowledge, but the challenge of not having clear definitions of correct behaviors to provide the necessary guidance still remains (Holmes; Bialik; Fadel, 2019, p. 127).

717. The type of technology used for implementing personalized learning will greatly depend on the learning objectives and what kind of governance decision will be affected. Therefore, we can also mention smart learning management systems, learning network orchestrators and digital games-based learning as other existing examples among the myriad of available technologies (Holmes *et al.*, 2018, p. 37–40).

718. Technologies have the potential to effectively implement personalized learning, and their promise is worth pursuing. However, they should not be considered a silver bullet that can solve all problems of current education systems, especially when they are still based on poor pedagogical approaches. All the current challenges they present should be taken into consideration within the decision-making process. Below, I will highlight the main challenges to children's rights to privacy and to the protection of personal data resulting from implementing personalized learning technologies within education.

8.3.4.2 Lack of robust evidence of their effectiveness

719. The efficacy of personalized learning tools has been demonstrated in some short studies, usually restricted to some contexts and universities (Holmes *et al.*, 2022). In the case of ITS, some meta-analysis concluded that, compared to one-to-one teaching, there was a negative effect size of -0.19, while compared to whole-class teaching it had an average effect size of 0.47 (Holmes; Bialik; Fadel, 2019). However, robust and independent evidence, especially focused on different groups and long-term effects, is still not available (Braun *et al.*, 2020; Dijck; Poell; Waal, 2018; Holmes *et al.*, 2018; Hooper; Livingstone; Pothong, 2022; Stringer; Lewin; Coleman, 2019).

720. On the contrary, some technologies might even reinforce poor pedagogical practices. While analyzing the 124 most-downloaded edtech mobile apps, for example, Meyer *et al.* (2021) highlighted that the majority showed lower-quality design, being distractive and repetitive, and provided minimal learning value. The research indicated that free applications scored lower due to disruptive advertisement and frequent, reward-driven feedback, which affected children's attention and learning.

721. Many edtech products replicate performed educational processes that were flawed since the beginning, incorporating those imperfections into their design: "a child recalls facts and answers; an application diagnoses and displays the outcome on a digital dashboard. Learning is recorded on some kind of scale as some kind of learning achievement" (Hillman, 2022, p. 7).

722. Kucirkova *et al.* (2023) highlight some reasons why edtech companies might refrain from designing their products according to evidence-based, scientifically sound research. Edtech companies are generally driven by Key Performance Indicators (KPIs), levels of funds raised, profitability, customer retention and/or product scalability. Another contributing factor is the gap between edtech funding and development: "[w]hile the investor and funding

community typically value impact metrics that are guided by scientific research principles, they do not have a unified approach to guide these efforts” (Kucirkova; Brod; Gaab, 2023, p. 1).

723. Therefore, based on the state-of-art and the current commercial incentives for personalized learning, there is little to substantiate the wide use in well-resourced classrooms apart from marketing pressure and groundless hopes by policymakers and administrators (Holmes *et al.*, 2022). In some regions, when there is a lack of qualified teachers, the argument for using these tools to support learning can be stronger. However, it should be viewed as a temporary measure, given that it addresses a consequence rather than the root cause (i.e. lack of appropriate investment in education) (Holmes *et al.*, 2022).

724. Edtech could have a more positive impact on education if certain conditions were in place, such as the development in tandem with researchers and pedagogues, focusing on learning principles (Kucirkova; Brod; Gaab, 2023, p. 1–2). In any scenario, the costs of implementing these technologies for other human rights should not be disregarded, especially the ones related to the rights to privacy and data protection.

8.3.4.3 Limits to personalization

725. Although it may seem counterintuitive, personalized learning technologies often do not empower students to make meaningful choices about their education. While it is supposed to let students take responsibility for their own learning, they usually lack awareness of how their choices are organized within the technology design and have limited influence on other students’ activities and the overall learning environment (Dishon, 2017, p. 282). Their choices are limited to when and how they will master a predetermined set of skills and personalization is restricted to the pathways to prescribed content (Miao *et al.*, 2021, p. 15). The learning outcomes are always the same and have been mandated by individuals who are often unaware of the student’s specificities (Kohn, 2015). Finally, it presupposes an educational dynamic where children are constantly under surveillance and can do little to revert this situation (Couldry; Mejias, 2019, p. 176).

726. The students’ learning path is not only constrained by the technology architecture but also by the interpretation of the data collected about them. In this context, the profiler does not necessarily adjust the learning paths to the student’s unique characteristics. Instead, after providing some initial data, students are conformed to the profiler’s standardized patterns. Personalization practices can then “homogenize” populations within sub-groups, and every student will be like others in fundamental aspects (Kohl, 2021). This is closely linked to the

debate on the individualization aspect of datafication and how the limits between individual and group data are blurred (see Section 8.3.1).

727. In the end, the mainstream available technology for personalized learning focuses on efficiently getting students to move quickly towards a learning outcome. “Real personalization, however, involves every student learning and achieving what they individually want to achieve, to what is called self-actualization. No current AIED system comes anywhere near helping students to achieve that” (Holmes, 2023, p. 62).

728. Another challenge is the way personalization is interpreted. As currently implemented, these technologies heavily emphasize the individual level of effort, which undermines the importance of both individual and social components of education. They tend to reduce the human contact among students and teachers and social interaction is often perceived as a secondary aspect (Miao *et al.*, 2021).

729. In a student-centered and project-based education, for example, children learn with each other by working together and developing their individual and collective autonomy. This means that while understanding concepts is undoubtedly a personal process, it is not limited to individual effort, and also requires working in a group (Kohn, 2015). This is essential for realizing a broader understanding of education, which includes community building and the development of social skills (Holmes, 2023, p. 62), as well as the cultivation of democratic citizens who are capable of shaping their learning environments and the larger society (Dishon, 2017, p. 282).

730. This is also related to the discussion on what level of standardization schools need to provide. On the one hand, personalization has the potential to address the complexity of learning and the specificities of each individual. On the other hand, some form of standardization might also be desirable to identify and narrow education gaps, as well as focus on collective achievements (Kucirkova, 2021).

8.3.4.4 Content filtering

731. Since personalization algorithms are based on inferences of users’ needs and interests, another possible result of this process may be filtering out some contents. In the words of Vaidhyanathan (2011, p. 182), “[l]earning is by definition an encounter with what you don’t know, what you haven’t thought of, what you couldn’t conceive, and what you never understood or entertained as possible. It’s an encounter with the other—even with otherness as

such”. Personalized learning can thus often be considered “the educational equivalent of filter bubbles” (Dijck; Poell; Waal, 2018, p. 125).

732. This is what Kucirkova (2022) calls the like-like logic of recommendation algorithms embedded in social media platforms, whereby similar content is suggested according to the user’s engagement. This works well when people are looking for a group that shares their niche interest, for example, but not necessarily for fostering new ideas and expanding viewpoints (Kucirkova, 2022, p. 225). “The mission of education should be precisely the opposite—ensuring that children have access to many different areas of knowledge, and that they can experiment with all these areas in open-ended and non-discriminatory ways” (Barassi, 2020, p. 80). The difficulty of encountering the unknown affects not only the individual as such and the possibility of learning new things but also society more broadly, as accepting and understanding different people and viewpoints are essential for democracy.

733. While personalized learning is often hailed as a way to enhance learning by tailoring the educational experience to the individual needs of each student, determining which information holds relevance or which content should be reinforced remains highly subjective and dependent not only on the pedagogical methods but also on the designers’ interests. Paradoxically, this has the potential to diminish student autonomy rather than enhance it. Finally, this logic also helps perpetuating power imbalances and inequities, further marginalizing underprivileged students (Holmes, 2023).

8.3.5 Student monitoring technologies

734. With the increasing adoption of digital technologies in schools, especially after the COVID-19 pandemic, it has become easier to monitor what kids do online and offline. This could be used, for example, to identify access to inappropriate content and online bullying, supervise students during an exam, ensure the safety of schools or monitor mental health, behavior or familiar issues. In this sense, a wide array of surveillance technologies have been increasingly deployed in schools, such as surveillance and facial recognition cameras, access control technologies, social media and student communication monitoring technologies, web filtering, weapon and metal detection etc.

735. Some enthusiasts argue that timely interventions could be implemented, for example, when students allow the sharing of conversations with advisors and professors. Special support can be provided to students dealing with dire situations, such as food insecurity. Personalized

emails could also be composed to help students with financial problems (Schaefer, [s. d.], n.p.). The edtech industry often markets these technologies based on two main narratives: that school and students' safety are at risk, which demands immediate attention, and that their products represent the optimal choice to solve the issue (American Civil Liberties Union (ACLU), 2023).

736. The emotional impact of fear on educators and the lack of resources and expertise to make decisions on the use of technologies can override statistics and science. There is still a lack of independent evidence about the efficacy of surveillance technologies in schools, and, in the case of surveillance cameras, there is already evidence showing that they actually do not prevent violence (American Civil Liberties Union (ACLU), 2023). The risks they pose to children's rights, however, are tangible, and the subsequent sessions will attempt to discuss some of them.

8.3.5.1 Behavior Monitoring

737. When it comes to behavior monitoring, a technology called Gaggle, widely used in the USA, could serve as an interesting example. Gaggle is a platform that uses a combination of AI technologies, such as ML, and human oversight to detect warning signs of potential crises among students, such as violence or self-harm, bullying, use of drugs, fighting, threats, or the presence of weapons on campus before they can escalate into tragedy.

738. Also on their list of worrisome words are LGBTIQA+-related ones such as "gay," "lesbian," and "queer." It can analyze every student's move, such as browsing history, social media notification, school email address, documents, interactions in the LMS, etc. (Haskins, 2019). By identifying these warning signs early on, Gaggle claims to help school administrators and teachers take preventative action and ensure the safety and well-being of their students (Who watches AI watching students? [Audio podcast episode], 2022).

739. A concrete example of its application was provided in the podcast "In machines we trust" (Who watches AI watching students? [Audio podcast episode], 2022). On a Friday evening, outside of school hours, a middle school student took out his Google Chromebook and began creating a document. The document contained the statement: "I'm tired of faking my feelings. I've got no one who loves me. Not even my family. My only choice left is suicide." Gaggle informed the school's principal of the situation, who then and contacted the student's home, while the assistant principal contacted the police. The student was later found walking towards a location where two other children had previously committed suicide by jumping in front of a train. All of this happened in just fifteen minutes.

740. Monitoring technologies like Gaggle typically work by analyzing and identifying students' online activities and content on school-provided devices, school networks, and especially on the adopted LMS. When monitoring software scans web traffic or specific applications, it can either scan the content and retain only the flagged material or keep all the material for future reference.

741. The algorithms can be based on natural language processing of keywords or phrases or use other types of AI. The service can also involve additional review layers, typically conducted by humans, as exemplified by Gaggle. In terms of response, it can vary depending on the system and what the school requires, ranging from content blocking and warnings to notifying parents, emergency services, and law enforcement agencies (Collins *et al.*, 2021, p. 4–6).

742. While these systems may seem promising in terms of identifying potential crises and ensuring student good behavior safety, “circumstances—in which there is a clear, imminent danger of a student about to harm themselves—are fortunately rare, and scanning for self-harm using monitoring systems often seeks to identify situations that are much more ambiguous” (Collins *et al.*, 2021, p. 4). These anecdotes must also be compared to the amount of erroneously flagged situations.

743. This prompts a discussion on how to accurately assess the success rate of such technologies. Since they are based on external behaviors, determining their preventive efficacy and long-term effects poses significant challenges.

For example, in one description of an incident involving interception of a student suicide plan, Gaggle asserted that “[t]he student now realizes the importance of being cautious [with] how you express yourself in an email.” One wonders, however, how much this student has been prevented from thoughts of self-harm as opposed to being deterred from ever again expressing her feelings about it in writing. If a student has other avenues to express her pain, she may get the help she needs; if, however, this particular means of communication was her only one, she may turn her negative feelings inward, internalizing the lesson that reaching out may yield only a police visit. What is more, the stigma and fear that a police visit may cause students is not discussed (Fedders, 2019, p. 1703).

744. Even in the USA, a country that leads the raking of school shootings²⁵, the chances of a student in primary or secondary education being shot and killed is 1 in 614 million, which is more than twice as unlikely as winning the top prize at the American lotteries Powerball or Mega Millions (American Civil Liberties Union (ACLU), 2023, p. 13). These statistics, together with the scant evidence that surveillance technologies are efficient to prevent violence

²⁵ According to Grabow and Rose (2018), the USA has had 57 times as many school shootings as the other major industrialized nations combined between 2009 and 2018.

and other undesired behaviors would already be enough to think twice before deploying them, especially when public resources are used.

745. However, on top of this, this kind of monitoring raises significant concerns regarding ethics, privacy and data protection issues, as well as the delicate nature of children's mental health. Although the intention behind such systems is usually noble, there are doubts about whether this approach is truly the most appropriate or effective in addressing the underlying issues students face.

746. For example, with filtering and blocking technologies, students can experience difficulties in completing assignments due to the lack of access to certain contents. Schools can also deploy subjective restrictions not always aligned with the promotion of human rights, such as filtering content related to LGBTQIA+ community, as stated before. Finally, there is always the risk of students circumventing the technology (Laird; Dwyer; Grant-Chapman, 2023).

747. One of the fundamental aspects of supporting children is establishing an environment of trust, where they not only feel comfortable confiding in adults about their struggles but are also able to seek for help elsewhere (American Civil Liberties Union (ACLU), 2023). By relying on surveillance mechanisms, there is a risk of creating a climate of suspicion and invasion of privacy, which could discourage children from seeking help or expressing their emotions openly. This constant monitoring can create a chilling effect whereby children avoid or limit their self-exploration. In the case of education, for instance,

[t]his can lead to students who do not feel that they can ask questions when they are questioning the behavior of adults in their life or of abusive partners or peers, who do not feel like they can explore resources if they are questioning their own gender or sexuality, or who are afraid to do research to understand the nuances of complex issues in their own lives. This self-repression can be damaging to students' mental health and well-being (Center for Democracy & Technology (CDT), 2022, p. 2).

748. It is also important to mention that “escalating a student's mental health treatment by hospitalising them or calling the police can be risky [... and] could worsen a student's symptoms” (Fasulo, 2019, as cited in Haskins, 2019, n.p.). The involvement of law enforcement authorities often obstructs students from accessing medical treatment and needlessly entangles them in the criminal justice system. This reinforces existing inequalities and perpetuates the school-to-prison pipeline. Groups who are already marginalized, such as students of color, students with disabilities, LGBTQIA+ and non-binary students, undocumented students or low-income students are the ones most likely to be flagged by monitoring systems and disproportionately referred to law enforcement or being harmed in another way (American Civil Liberties Union (ACLU), 2023, p. 25 et seq.; Collins *et al.*, 2021, p. 20).

749. To create a sustainable and holistic impact on students' well-being and foster good behavior, it is essential to invest in resources that address the broader societal and environmental factors affecting children's safety and mental health. Surveillance technologies predominantly attempt to address the aftermath rather than tackling the underlying factors that contribute to issues students face.

Table 5 – Gaggle and its impacts on privacy and mental health

750. During the pandemic, a 13-year-old transgender person from Minneapolis, USA, experienced exacerbated gender dysphoria and emotional distress. This culminated in a suicide attempt, leading to hospitalization and subsequent outpatient psychiatric care. The student eventually improved and decided to reflect on this episode and how music therapy helped him cope in a school assignment. The document was flagged by the monitoring system Gaggle, especially because of the word suicide, and triggered school intervention. His mother was called to learn about the situation without considering the context of the student's mental state and the meaning of the assignment (Keierleber, 2021).

8.3.5.2 e-Proctoring

751. Apart from technologies used to monitor children's well-being and unwanted behavior online, other technologies to support teachers have been heavily introduced within the school environment, especially with the COVID-19 pandemic. It includes, for example, software to detect plagiarism and services that monitor students during online test-taking (e-proctoring). Proctorio, for example, is a well-known software that provides services such as identity verification, automated and live proctoring, plagiarism detection, and content protection. It uses

gaze-detection, face-detection and computer-monitoring software to flag students for any "abnormal" head movement, mouse movement, eye wandering, computer window resizing, tab opening, scrolling, clicking, typing, and copies and pastes. A student can be flagged for finishing the test too quickly, or too slowly, clicking too much, or not enough. If the camera sees someone else in the background, a student can be flagged for having "multiple faces detected." If someone else takes the test on the same network — say, in a dorm building — it's potential "exam collusion." (Harwell, 2020, n.p.).

752. This information is then used to assess a student's conduct throughout the exam and detect any behavioral patterns that could be interpreted as cheating. For instance, the level of suspicion in relation to a student increases if their gaze deviates from the screen for an extended period. The algorithm, occasionally in collaboration with a human proctor, determines which

individuals are deemed suspicious and identifies who is considered to be engaging in cheating behavior (Watters, 2020).

753. According to some students, the system sometimes mistakes harmless actions like reading questions out loud or looking away as a response to thinking as signs of cheating. The possibility of failing can be an extra factor of anxiety, especially when it relates to movements the student cannot control. Professors have the power to decide which student behavior is monitored and choose to ignore the system's findings, but there is no guarantee. In a context where teachers have no direct access to the student's behavior, it is common to assume that the technology is objective and has greater monitoring capabilities, meaning that everything it detects aligns with reality. Therefore, in order to defend their honesty, students might have to prove that the technology got it wrong (Harwell, 2020).

754. Apart from the cognitive bias, the technology was also accused of not taking into account some student's living conditions—such as the fact that some live in dormitories or houses with many people—and of racial bias as it would not recognize black faces more than half of the time (Mitchell, 2021).

755. Proctoring and other student monitoring technologies have in common the fact that the environment being created in schools is focused on control and mistrust, frequently using a narrative of care. The very place that should foster the exploration of knowledge about the world and oneself and cultivate ethical, responsible citizens prepared for the swift changes in society is, in fact, doing the complete opposite.

8.3.6 Learning Analytics and further use of data

756. The typology developed in Chapter 1 includes not only edtech used for providing education directly but also technologies used to *learn about learning*. The data and analytical techniques used for this purpose are generally the same as for providing education, but the focus is on understanding “how learners learn, learning progression, or which learning designs are effective [...]” (Holmes *et al.*, 2022, p. 19). This is also called learning analytics.

757. As discussed above, personalized learning and other ways of implementing data-driven technologies for providing education collect an immense amount of students' data. A single session of interaction between a child and an edtech could generate around 5 to 10 million actionable data points per student, with education being considered the most “data-minable industry” (Data mining of school kids, 2012).

758. However, this digital footprint does not only help students learn better and personalize their experience. Apart from processing the collected data, AI tools will produce new data that could be fed again into the AI model (Laet, 2023, p. 50), especially data on how students learn and behave. By analyzing student behavior and engagement patterns, developers can train their AI models to make predictions about future trends that are considered more accurate. This information enables businesses to make informed decisions, such as forecasting demand for educational products and services, thereby informing strategic planning and resource allocation.

759. The constant data cycle presupposes this step in order to improve the algorithm and then personalize experiences based on group data. However, this also means that students' data could be used for other purposes not necessarily related to their learning process. Education data can provide insights into the knowledge, skills and competences of individuals and groups, as well as serve as proxies for various other situations. They can inform decisions across a wide range of areas and are valuable for different stakeholders, such as companies, data brokers, social scientists, political parties and the government (Chakroun *et al.*, 2022).

760. For instance, employers can use these data to make hiring decisions. A candidate's background and performance in school are often proxies for the candidate's suitability for the role and potential success. Applicant Tracking Systems (ATS) is one of the technologies used in a "talent acquisition" process, which has evolved to include "AI-based recruitment tools, skills assessments, candidate relationship management, onboarding, and even internal talent marketplaces" (Gallagher *et al.*, 2023, p. 7).

761. There is a growing interest in skills-based hiring in the market, meaning that prospective job candidates are assessed based on their skills rather than traditional degrees (Gallagher *et al.*, 2023, p. 16). These skills are usually captured and communicated through digital credentials, which "promise to make education more relevant by documenting learning in a way that empowers people to plan, track, and share their accomplishments in a secure and verifiable way" (Understanding Digital Credentials Building Value from an Ecosystem of Open Standards, [s. d.], n.p.).

762. Comprehensive Learner Records (CLR), for example, are digital portfolios that promise to provide a more holistic and accurate representation of a student's skills, knowledge and abilities. They not only focus on credits and grades but provide detailed information of student's learning experiences (Understanding Digital Credentials Building Value from an Ecosystem of

Open Standards, [s. d.], n.p.). CLR can include any kind of data related to a student's education or skills.

763. Commercial uses of education data are also of interest of edtech and other third-party companies. The profile built through data gathered by persistent identifiers that track children across multiple devices could be used for advertising or other commercial purpose. In a research carried out by Human Rights Watch that analyzed 73 edtech apps, 56% were found to collect children's advertising IDs²⁶, and none of them allowed children to opt out of the tracking activities (Human Rights Watch, 2022, p. 24–26). This clearly shows the surveillance element of these technologies in children's lives.

764. Fourteen of the analyzed applications also had access to information like the Wi-Fi Media Access Control (MAC) address or the International Mobile Equipment Identity (IMEI), “two persistent identifiers that are so strong that a child or their parent cannot avoid or protect against their surveillance even if they take the extraordinary step of wiping their phones or performing a factory reset” (Human Rights Watch, 2022, p. 27). Lastly, of the 163 apps examined by Human Rights Watch, 80% were found with embedded tracking technologies built by Google, which gives the company access to children's data from many different sources (Human Rights Watch, 2022, p. 86).

765. The identifiers referred to above are just an example of the broader surveillance that children are put through because of commercial activities. Others include tracking where children are, who they know, how they deal with content online and what they do in the classroom often in an unnecessary and disproportional way. Many continue to track children outside the classroom, especially when the same device is used for other personal activities. Human Rights Watch also identified that “most EdTech companies did not disclose their surveillance of children and their data; similarly, most governments did not provide notice of these practices and their risks to students or teachers when announcing their endorsements of EdTech platforms” (Human Rights Watch, 2022, p. 41).

766. Even when children's data are not used for advertising purposes, other commercial interests can still be identified that would justify surveillance. First, children represent a

²⁶ “An advertising ID is a persistent identifier that exists for a single use: to enable advertisers to track a person, over time and across different apps installed on their device, for advertising purposes. For those using an Android device, this is called the Android Advertising ID (AAID). An AAID is neither necessary nor relevant for an app to function; Google's developer guidelines stipulate that app developers must ‘only use an Advertising ID for user profiling or ads use cases’” (Android for Developers, as cited in Human Rights Watch, 2022, p. 24).

significant market segment with their own distinct needs. By trying to understand their behavior and preferences through data analysis, companies can tailor their products and services to better adapt them to this specific demographic.

767. Moreover, collecting children's data, or even being present in their lives early on, can contribute to building a loyal customer base for the future. By establishing a relationship with children at an early age and getting them used to their products, companies can potentially retain them as customers for many years, especially when the business model depends on scaling. This is particularly advantageous for companies offering products or services designed for children, such as toys or educational materials, and is especially the case when they are offered free of charge. Early experience with a brand or product could increase the likelihood of continued usage as children grow older and become more independent consumers. This is especially true when the brand creates a feeling of nostalgia in the user, which increases brand loyalty (Mondragon Ruiz, 2021).

768. Children also play a crucial role in influencing family purchasing decisions (Chaudhary, 2016). While parents often make the final choice, children strongly influence those decisions. They may request specific items, such as toys, clothing, or food, prompting parents to fulfil their wishes.

769. Education data can also be instrumental in enhancing products and services. Companies in the edtech sector can use data on student performance and behavior to develop new features that improve learning outcomes and engagement. Children's interactions with edtech are thus providing not only technical knowledge about how a product works but also business intelligence about how a product is used. These data can be used to improve edtech products and other offerings within the companies' portfolio, including job, health, and dating apps. Therefore, the remaining question is whether student data should be used for these purposes and whether the latter are being prioritized over children's educational goals and well-being.

770. Beyond the issues concerning how companies are using data, we should also reflect on the consequences of this transfer of knowledge from the public to the private sector. Indeed, this can directly impact children's future opportunities, determining the universities they will attend, the jobs they will secure, and the services they are entitled to. However, the amount of information that private actors have access to can also directly shape our economies and society, leading to an asymmetry of information and consequential power imbalance that can undermine democracy and the rule of law.

771. Due to the proprietary aspect of algorithms and the information they create (even if it is created with children's own data), states have less information about public education than the private actors themselves, which directly impacts public policies. Ultimately, it can lead to and reinforce the lack of digital sovereignty, reducing the autonomy of states to determine their digital destinies, the policies and legislation they will enact, and the technology they will have access to, which is at the heart of data colonialism practices.

Interim conclusion

772. This chapter aimed to provide an overview of the main challenges that edtech poses for children's rights, especially with regard to their rights to privacy and the protection of personal data. The first part of the chapter focused on horizontal risks presented by AI, given that these systems are present in the majority of today's edtech.

773. I started by examining the process of datafication itself and the issues stemming from reducing and abstracting reality into quantifiable variables. I discussed the operations of AI systems, noting the significant volume of data required for training and functioning, as well as the repurposing of data, which already poses challenges to the principles of purpose limitation and data minimization, as well as other basic data protection rules such as the need for a legal basis.

774. I have emphasized the concerns surrounding data generation within AI systems and how the inferences drawn can be tainted with bias and significantly affect individuals' control over their data. This calls for a greater focus on AI systems' outputs and the development of more tools for controlling personal data, such as the right to reasonable inferences.

775. The challenges related to decision-making based on the inferences made by AI systems have also been discussed, including those related to profiling, predictions and human interpretation of data. We have seen that algorithmic predictions have the potential not only to cement past circumstances, thereby impeding social mobility, but also to influence future outcomes, as patterns are not simply recognized but actively shaped by these predictions.

776. Building on the typology developed in Chapter 1, I also focused on some issues related to specific technologies, namely personalized learning, student monitoring technologies and learning analytics. After discussing its definition and historical context, I highlighted that although promising, personalized learning through technologies may still not be fit for purpose,

considering its risks. There is a lack of robust evidence demonstrating its positive impact on learning outcomes or other educational goals. Moreover, I emphasized how these technologies often overly focus on individual efforts at the expense of social components of education. I have also shown that the aspects that can indeed be personalized are limited, and these technologies can be, on the contrary, constraining student's learning paths and choices by predefined parameters, limiting their autonomy and potential for being whomever they want to be.

777. Although student monitoring technologies are often created with noble and legitimate aims in mind, such as dealing with student's mental health and preventing cheating, they frequently raise concerns related to surveillance. Surveillance mechanisms can create a climate of suspicion and invasion of privacy, hindering students from seeking help or expressing their emotions openly. It also creates a chilling effect that will affect children's development and learning (as have been discussed in Chapter 4). The focus on control and mistrust, under the guise of care, can paradoxically undermine the development of ethical, responsible citizens and perpetuate biases and inequalities, disproportionately impacting marginalized groups. This is even more serious when there is still scant evidence of these technologies' efficiency to tackle violence and other kinds of behavior within schools.

778. Lastly, I have also focused on the use of technologies for learning about education. I discussed how learning analytics analyze data from student interactions and AI models to generate new data that can inform the learning process, particularly regarding how students learn and behave. This enables companies to refine their AI models for more accurate predictions about future trends.

779. However, these data are often also used for purposes beyond the scope of education. There is a growing trend of using data for skills-based hiring and comprehensive learner records to provide a more holistic representation of student's skills and learning experiences. Students' data are also used for other commercial purposes, such as targeted advertising, creating a loyal customer base from an early age and developing other products. This raises concerns about limiting children's future opportunities, power imbalances, data protection and the erosion of digital sovereignty.

Chapter 9. Google Workspace for Education

780. This chapter aims to present what Google Workspace for Education is, its main features, and how it fits into the broader context of Google's business model. As described in the introduction, there are several reasons why Google Workspace for Education was chosen as a case study for this thesis. In summary, Google was a pioneer in DDBM on the scale that we currently know, which have been replicated across the digital environment, including by other edtech platforms; Google Workspace for Education is widely adopted worldwide; and Google is deeply involved in a broader network of data sharing, owing to its market power. Therefore, studying Google's dynamics can provide a framework to understand other commercial edtech platforms in the current digital economy and their impacts on children's rights to privacy and data protection.

781. With the COVID-19 pandemic and the further expansion of Google's deployment, a significant number of decisions made by competent authorities in Europe regarding its operations and the impact on personal data protection has surged. This is yet another reason to understand in greater detail the effects of this technology and gain insights from what has been found by the authorities.

9.1 What is Google Workspace for Education

782. On August 28, 2006, Google announced its web-based office suite named Google Apps for Your Domain combining various productivity tools (Statz, 2006). Although these tools were already accessible to individual customers, the package was primarily tailored to organizations aiming to provide them to their employees (Flynn, 2006). At the moment of its introduction, the suite encompassed GMail, instant messaging, Google Calendar, and a web page creation tool (Google, 2006b).

783. In October of the same year, Google announced Google Apps for Education, an initiative that would tailor the use of Google Apps for Your Domain for education institutions. This included new features such as the partnership with Blackboard—that would integrate Google enterprise search technology for schools and the Blackboard Learning System with Google Scholar—as well as the launch of an Application Programming Interface (API) that would simplify the process for organizations to integrate with Google Apps for Education (Google, 2006a). Later in 2006, Google purchased YouTube (Sorkin; Peters, 2006).

784. Over time, additional tools were introduced, including Google Spreadsheets, and Google Docs in 2007 (Google, 2007), as well as Google Presentations and Google Sites in 2008 (Google, 2008). In 2010, Google launched the Google Apps Marketplace that enabled Google Apps administrators to purchase integrated third-party cloud applications (McMullan, 2010). Google Drive was then introduced in 2012 (Johnston, 2012).

785. The beta version of Google Classroom was only launched in 2014 and was available for some selected schools (Magid, 2014). In 2015, a mobile version of Classroom was launched, together with the Google Classroom API, and a share button for websites (Perez, 2015). Google Apps for Education was renamed Google Suite for Education in September 2016 and later in 2020 as Google Workspace for Education (Google, 2020; Perez; Lardinois, 2016).

786. While it was not initially created to be an LMS (Lazare, 2021a), it constantly increased its features over time and teachers started to use it as a “hub” for educational content. Because of the pandemic, Google Classroom has increased from 40 million to 150 million users (Lazare, 2021b), making it one of the most used edtech worldwide. According to LearnPlatform, which publishes a regular Edtech Top 40 list of the most used edtech products in primary and secondary education in the USA, Google products took 8 of the top 10 spots in 2022 (Palmer, 2022).

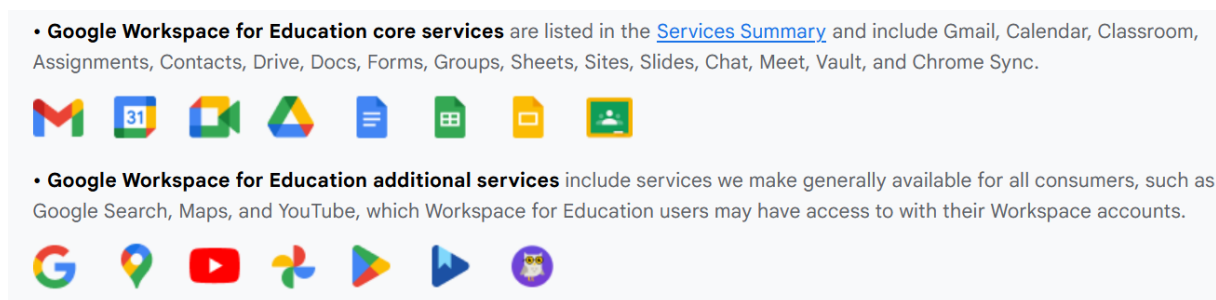
787. Anyone with a Google account can use Google Classroom, but to use Google Workspace for Education as a suite of applications, a school account is necessary. After being approved for Google Workspace for Education, schools can add users to their domains, set up the available apps, and use advanced features, such as mail migration.

788. Schools can choose from different editions of the application suite. With the Google Workspace for Education Fundamentals, they can access the core services, such as Classroom, Docs, Sheets, Slides, Forms, etc. The Google Workspace for Education Standard has the same features as the Fundamentals but also includes premium security and information technology features. The teaching and learning upgrade provides premium teaching and learning features to be added such as third-party add-ons, Microsoft Word support, call transcripts, YouTube Live Streams, among others. Finally, the Education Plus includes all features in the Standard version and the Teaching and Learning Upgrade. The Fundamentals edition is available at no

cost to schools, while the premium features demand annual subscriptions (Google, 2023b, 2023a). The main core²⁷ and additional²⁸ services are depicted in the figure below:

789.

Figure 6 - Google Workspace for Education's core and additional services



Source: Google (2023f)

790. Apart from the application suite, Google also provides Google Chromebooks for Education, a simple and affordable laptop based on web applications using Google Chrome browser (Google, 2023e; Magid, 2014; Upson, 2011), as well as smart whiteboards to use the Jamboard application (Google, 2023i).

791. Educators using Google Workspace for Education can participate in Google Educator Groups (GEGs), which bring together “teachers from the same region, in person or online, in a forum where they can share, collaborate and support each other to effectively leverage technology with students” (Google, 2023h, n.p.). Each group is organized by a volunteer GEG leader who despite not being formally linked to Google, acts as marketer for Google products (Sujon, 2019).

²⁷ The list of core services include: Client-Side Encryption, Cloud Identity Services, Duet AI for Google Workspace, Enterprise Data Regions, Gmail, Google Calendar, Google Chat, Google Cloud Search, Google Contacts, Google Docs, Google Sheets, Google Slides, Google Forms, Google Drive, Google Groups for Business, Google Jamboard, Google Keep, Google Meet, Google SIP Link, Google Sites, Google Tasks, Google Vault, Google Voice, Google Workspace Assured Controls, Google Workspace Migrate, Meet Global Dialing, Workspace Additional Storage, and Workspace Add-Ons (GOOGLE, 2023g).

²⁸ The list of additional services include: Applied Digital Skills, Assignments, Blogger, Brand Accounts, Campaign Manager 360, Chrome Canvas, Chrome Cursive, Chrome Remote Desktop, Chrome Web Store, Classroom, CS First, Early Access Apps, Experimentnal Apps, FeedBurner, Google Ad Manager, Google Ads, Google AdSense, Google Alerts, Google Analytics, Google Arts & Culture, Google Bookmarks, Google Books, Google Business Profile, Google Chrome Sync, Google Cloud, Google Colab, Google Developer, Google Domains, Google Earth, Google Fi, Google Groups, Google Maps, Google Messages, Google My Maps, Google News, Google Pay, Google Photos, Google Play, Google Play Console, Google Public Data Explorer, Google Read Along, Google Search Console, Google Takeout, Google Translate, Google Trips, Location history, Looker Studio, Managed Google Play, Material Gallery, Merchant Center, Partner Dash, Pinpoint, Play Books Partner Center, Programmable Search Engine, QuestionHub, Scholar Profiles, Search Ads 360, Search and Assistant, Socratic, Studio, Third-party App Backups, Tour Creator, and YouTube (GOOGLE, 2023g).

792. Google also offers training and certification programs to educators. Online training courses are available at no cost for teachers so they can learn the fundamentals of the tools. Educators can then become certified teachers by participating in two levels of exams designed to assess educators' abilities to use Google Workspace for Education (Google, 2023f). After getting certified as a Google Teacher, it is possible to become a certified trainer in order to train fellow teachers on Google tools (Google, 2023c, 2023l), as well as a certified innovator, which encourages teachers to lead so-called "transformative projects" proposed by Google.

9.2 The main features of Google Workspace for Education

793. As explained above, Google Workspace for Education is a suite of applications tailored for teaching and learning, which attempts to resemble the processes that occur face-to-face within schools. The central hub for activities within schools is the Google Classroom where other applications can be embedded or linked. Within Google Classroom educators can create and manage classes, assignments, and grades; give direct and real-time feedback; post announcements; engage with students in discussion fora; start video meetings; among others.

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

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

796. Classroom analytics provide educators with insights into assignment completion rates, grade trends, and Classroom adoption, with the possibility to delve into the individual student level to better provide support (Sinha, 2024). Additionally, generative AI is increasingly being

integrated into Google Workspace for Education. For example, Duet AI is designed to assist teachers across the suite's applications, aiding them in drafting lesson plans in Google Docs, generating images in Google Slides, or building spreadsheets in Google Sheets.

797. Although occurring through digital ICT, the educational processes enabled by Google Classroom still mostly reproduce a hierarchical classroom structure, as well as a behaviorist approach to learning (Gleason; Heath, 2021, p. 33). Within the pedagogical domain, the mechanisms and structures of formal schooling are said to be abstracted to fit a predefined template for participation. According to Perrotta *et al.* (2021, p. 107) this is done by the notion of a “doubly articulated pedagogy”, which encompasses three main components:

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

798. Even with Google stating that teachers should have a more significant role than technology (Langreo, 2023), these components mean that important decisions taken in relation to how the platform is designed and works are delegated to developers and often exclude educators (Perrotta *et al.*, 2021, p. 108). One illustrative example is provided by Jonathan Rochelle, the former director and product manager of Google, who was involved in the development of Google Classroom and other applications within the current Google Workspace for Education Suite. Referring to his children in a speech at an industry conference, Rochelle said: “I cannot answer for them what they are going to do with the quadratic equation. I don’t know why they are learning it [...] and I don’t know why they can’t ask Google for the answer if the answer is right there” (Singer, 2017).

799. More than the content of the statement itself, what matters is what can be implied. The practice of memorizing facts is long criticized by more progressive pedagogies. However, more deeply, it suggests that Google has effectively become the arbiter of relevant knowledge and the ways to access it (Krutka; Smits; Willhelm, 2021, p. 427). It becomes able to determine whether something is useful and worth teaching or not, implying that any information obtainable through a Google search is deemed irrelevant to learning. Rather than prioritizing the process of critical thinking and the methods required to arrive at the correct answer, only the result is considered significant (Bäcke, 2022, p. 60), reinforcing the *learnification* of education paradigm. This concern might escalate with the increasing use of generative AI in education.

800. Moreover, especially with the dominance of its search engine, Google is influencing human memory, acting as an index and as a filter (Vaidhyanathan, 2011, p. 174–179). It changes what we humans choose to forget or remember, which can be a challenge when it comes to how people are educated and what kind of personal data are available not only for Google but also for third parties.

801. Google's role within education is only possible because of Google's broader role within the current society. Google's mission is defined as “to organize the world's information and make it universally accessible and useful” (Google, 2023j). Hillis, Petit, and Jarrett (2013, p. 6) argue that this power has given Google a consecrated status, both in the sense of being sanctioned by law, custom, or usage, and of something set apart by being hallowed, sacred, or divine. This “sacred” power and all the benefits that the technology provides mesmerizes educators, as well as public administrators.

9.3 The role of Google Workspace for Education within Google's business model

802. Efforts to quantify human behavior and use data to improve businesses have existed for centuries. Data have been used to inform internal decision-making processes and understand customers' preferences. Examples of early DDBM include selling customer profiles by data brokers, targeting with personalized direct mail campaigns, and customer loyalty programs.

803. Systematizing, understanding, and finding patterns in data was very labor intensive. However, advancements in the technological landscape (such as the advancement of computer processing capabilities, the spread of smartphones and connected devices, the rise of cloud computing technologies, and the improvement of AI systems) have made it more cost-effective to collect, store and process vast amounts of data, including personal data. Although the infringement of the rights to privacy and data protection was already an issue in the early adoption of DDBM, the so-called “data revolution” has taken it to another order of magnitude.

804. In this sense, Zuboff (2019) explains how Google had a key role in fostering the current DDBM, and compares their importance to how the Ford Motor Company and General Motors fostered mass-production-based managerial capitalism. Since the beginning, Google search queries produced a great amount of metadata (such as the number and pattern of search terms, how a query is phrased, spelling, punctuation, dwell times, click patterns, and location). Initially, these data were ignored by the company, but the work of Amit Patel led to the realization that “the continuous flows of collateral behavioral data could turn the search engine

into a recursive learning system that constantly improved search results and spurred product innovations such as spell check, translation, and voice recognition” (Zuboff, 2019, n.p.).

805. Through what the author calls the behavioral value reinvestment cycle, behavioral data were being used only to improve the user’s experience in the form of improved services (Zuboff, 2019). At this stage, Google’s vision of a search engine still repealed the use of advertisement for its funding, which was elaborated on a foundation paper written by its founders:

[W]e expect that advertising funded search engines will be inherently biased towards the advertisers and away from the needs of the consumers. Since it is very difficult even for experts to evaluate search engines, search engine bias is particularly insidious [...] This type of bias is very difficult to detect but could still have a significant effect on the market. Furthermore, advertising income often provides an incentive to provide poor quality search results. [...] [W]e believe the issue of advertising causes enough mixed incentives that it is crucial to have a competitive search engine that is transparent and in the academic realm (Brin; Page, 1998, p. 18–19).

806. Nevertheless, with the implosion of the “dot-com bubble” and the need to find a business model to sustain Google’s activities, these “collateral” data started to be used to improve the profitability of advertisement, what Zuboff (2019) calls the discovery of *behavioral surplus*. Advertisements have always been based on the idea of delivering “a particular message to a particular person at just the moment when it might have a high probability of actually influencing his or her behavior” (Zuboff, 2019, n.p.). Before the use of the behavioral surplus, advertisements on the internet were based mainly on the use of keywords or content, not on the specificities of a particular user. What Google presented as a solution was the increase of the “relevance” of advertisement based on deducing user’s needs and wishes through their behavioral data. These data could be directly given by the user, observed, or inferred (Hof, 2017; Zuboff, 2019).

807. What is important for this thesis is that

Google’s invention revealed new capabilities to infer and deduce the thoughts, feelings, intentions, and interests of individuals and groups with an automated architecture that operates as a one-way mirror irrespective of a person’s awareness, knowledge, and consent, thus enabling privileged secret access to behavioral data. A one-way mirror embodies the specific social relations of surveillance based on asymmetries of knowledge and power. (Zuboff, 2019, n.p.).

808. The internet, which in the mid-1990s was primarily perceived by companies as a marketplace for the sale of goods and services, evolved into the perfect place for harvesting user data, strengthening the development of tracking technologies, and leading the commercial web down a path of surveillance and dire power asymmetries (West, 2019).

809. Google is a pioneer when it comes to processing data for further use, especially for marketing, and it has influenced the creation of the current widespread business model in the digital environment. In order to scale and gather more data, so predictions were more “accurate”, there was a need not only to attract more users but to be ever more present in users’ lives through different means. Therefore, Google started to expand to other areas beyond search such as providing services for schools.

810. One of the characteristics that makes the use of Google Workspace for Education attractive is that it provides the majority of its services free of charge and some for an affordable fee. An interesting finding from the Privacy Company’s DPIA within the Dutch case, which will be described below in Chapter 10, was that apart from the possibility to store specific consent data within the EU (which indeed is very important to comply with data transfer rules and foster digital sovereignty) and the provision of additional security management options, there were no other significant distinctions in data protection between the free and paid editions of Google Workspace for Education (Nas, Sjoera; Terra, 2021, p. 5).

811. In the beginning, Google would allow advertisements to be displayed within the suite, which were also based on students’ and educators’ email content. The scanning and indexing would happen even when advertisement options were turned off. However, after a lawsuit in 2014 that questioned whether Google’s practices were in compliance with the Family Educational Rights and Privacy Act (FERPA - USA) (Herold, 2014), Google decided to permanently remove “the ‘enable/disable’ toggle for ads in the Apps for Education Administrator console”, as well as “all ads scanning in Gmail Apps for Education” (Bout, 2014, n.p.).

812. The lack of advertisement within the suite and the non-use of collected data for advertising purposes on other platforms, however, do not pose a threat to Google’s business model and the potential revenue derived from Google Workspace for Education. Although there may be little or no direct monetary exchange between end users and digital platforms, the former still have to give up on something to sustain the market.

813. O’Reilly *et al.* (2023) call this platform model Algorithmic Attention Rents. According to the authors, rents are related to control over a scarce factor of production, which allows its holder to profit above what would be normally achievable in a competitive market. Rather than the result of productive improvements to grow the economy, rents represent a reallocation of economic value from one party to another due to market power. In the case of digital platforms,

the scarce factor would be the attention of their users and this kind of rent would be linked to the ability to distort organic results. The allocation of attention within platforms will then drive value allocation. In the authors' understanding, data would be the means to more effective attention allocation and not necessarily an end in itself (O'Reilly; Strauss; Mazzucato, 2023, p. 4–5).

814. However, “[t]he current increase in rents is a major contributor to increased inequality, less vibrant entrepreneurial ecosystems, and lower levels of productivity growth and investment in modern economies” (O'Reilly; Strauss; Mazzucato, 2023, p. 3). What is mistakenly understood as “for free” or relatively cheap may be explored in the expense of individual and collective externalities that should also be factored in (Trzaskowski, 2022, p. 234), such as issues related to competition, data protection, procurement, and children’s best interest more broadly.

815. One of the main arguments currently used by Google to promote its products is the absence of advertisements within Google Workspace for Education Core services, as well as the assurance that user data is not collected for advertising purposes. Consequently, delving deeper into this discussion is essential to grasp Google’s economic motivations behind offering this suite.

816. After analyzing the institutional logic behind the involvement of the main transnational technology corporations in education, Patil (2023) concluded that financial gain was their main drive. This could take the form, for example, of brand recognition, market development, or workforce development and all these aspects can be recognized in the Google Workspace for Education case.

817. First, Google’s marketing strategy heavily relies on brand loyalty and recognition. The focus then is not necessarily on immediate transactions but on profitable growth in the long term. The so-called customer lifetime value (CLV) is often used as a metric to measure, as the company puts it, “the total value a business receives from a single customer over their entire relationship, is an ideal way to acquire, develop, and retain the most valuable customers for business growth” (Fader; Hoyne, 2021, n.p.). This includes, for example, providing their services for free to attract new audiences, creating early exposure to the products to create familiarity, encouraging life-long learning, building community experiences, etc.

818. It also encompasses expanding their business to increasingly more areas. In the case of Google, the focus of their products go from search to education, shopping, patents, finance,

communication, productivity, maps, healthcare, and operational systems. Veliz (2022) contends that these are not necessarily products designed for people, but rather new ways to collect more and different data from them.

819. Second, Google Workspace for Education encompasses two different kinds of services, as explained above. Core services are the main services offered to schools and include, Google Classroom, Calendar, Docs, Sheets, and Gmail (Google, 2023k, 2023g). Additional Services, like YouTube, Google Maps, and Blogger, “are designed for consumer users and can optionally be used with Google Workspace for Education accounts if allowed for educational purposes by a school’s domain administrator” (Google, 2023g, n.p.). This differentiation is crucial, as it determines how students’ and educators’ data will be processed by Google.

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

821. It is unclear how students’ data flow from one kind of service to another while being used throughout school activities, particularly when they are embedded within each other. As we will see in the case of the Netherlands, the agreement made between the schools and Google stipulated that when embedded in Google Classroom, YouTube videos would adhere to the same rules as the core services. However, it is not possible to ascertain whether this is also the case for other jurisdictions.

822. Google also encourages parents and guardians to create a second account for the child, which can be linked to the school account through the Family Link, as this would empower them to set parental controls across accounts (Hooper; Livingstone; Pothong, 2022). However, what remains unclear is that this action might inadvertently prevent the child from benefiting from the protective measures instituted by the school within the school account.

823. Therefore, the problems persist in the majority of products and the core services can be serving as a bait to acquire more users and as a pathway for children to move from privacy-friendly environments to data-harvesting ones (Hooper; Livingstone; Pothong, 2022, p. 55). A user experience study conducted by Hooper *et al.* (2022) discovered that the seamless user interface blurs the distinctions between core and additional services. This results in users easily

transitioning between them without being aware of the differences in terms of data protection and the associated consequences.

824. A third aspect that should be considered is that to support Google's commercial interests, data do not need to be processed only for targeted advertising. Google can use the data to refine and enhance their products and services. This involves analyzing user data to gain insights into consumer behavior, preferences, and trends. By understanding how users interact with their applications, Google can improve design, develop new features, and tailor their services to better meet the needs and desires of their (future) customers. Additionally, data can also be used for improving and training Google's AI tools. In this sense, children's data become valuable to understanding preferences within a specific generation, family dynamics, future trends, etc.

825. A fourth important aspect is that Google can access children's data indirectly, through data shared by other edtech, due to its dominance over the digital realm. In a study of 163 edtech products, Human Rights Watch discovered that 80% of them were found with at least one embedded Google software development kit (SDK). The NGO discovered that edtech companies would in some instances share children's data with Google's advertising division (Human Rights Watch, 2022). Its "vertically integrated chain of platforms and algorithms" (Couldry; Dijck, 2015, p. 4) facilitates this process, as Google currently dominates the advertising technology (adtech) market both in terms of selling advertising space on its own websites and apps and being an intermediary between advertisers and publishers that can supply advertising space. This is what led the European Commission to send a Statement of Objections to Google over abusive practices in June 2023 (European Commission, 2023a).

826. A fifth aspect to be considered is the integration of Google Workspace for Education with other applications through the Google Classroom API. Integration and interoperability are also fundamental for expanding Google's business model, maintaining its relevance, and increasing its adoption and customer retention. With the API, Google can attract developers and software providers, outsourcing the task of expanding the platform's functionalities to "enrich the classroom experience, as long as they remain aligned with the overarching data ontology" (Perrotta *et al.*, 2021, p. 103).

827. The amount of data that it has access to also increases. The use of the API "allows Google to monitor and regulate how data are being exchanged, and how functionalities and their associated practices are integrated in the Classroom experience" (Perrotta *et al.*, 2021, p.

103). This gives Google a powerful role of gatekeeper for the edtech industry, setting the rules for third-party providers to integrate with Google Classroom and share data between them (Williamson, 2021).

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

Interim conclusion

829. To discuss the challenges posed by Google Workspace for Education regarding children's data in the following chapters, this chapter aimed to describe what it is and how it operates, as well as its relationship to Google's broader business model. It emphasizes the importance of understanding Google's dynamics as a framework for the wider landscape of commercial edtech platforms and their implications for children's rights to privacy and data protection.

830. Key milestones in the development of Google Workspace for Education, particularly within Google Classroom, have been highlighted. We have observed that the design of Google Classroom and the broader pedagogical possibilities within Google Workspace for Education are still tied to a traditional and hierarchical vision of the classroom, reinforcing a behaviorist and quantitative approach to education that benefits from the phenomena of datafication and the learnification of education.

831. More importantly, this vision is aligned with the specific needs of Google's business model. Even though the application suite is free, Google still has very specific commercial reasons for keeping children within its ecosystem, including brand loyalty and recognition; blurred boundaries between its services with varying levels of data protection; indirect access to children's data via other platforms; and the use of data for other commercial purposes, even if not for targeted advertising.

832. Overall, Google serves as an important case study precisely because it is typical and representative of the mainstream business model in the digital economy. It shows how big tech companies are increasingly influential in significant decisions in education, including what children should learn, how they should learn it, and with what tools. The growing integration

of AI in the educational environment reinforces this notion, and if not adopted critically and for specific purposes within a broader pedagogical strategy, it could render teachers increasingly irrelevant. This educational perspective and the technologies used to implement it directly impact the quantity and quality of data processed by edtech platforms.

833. This reinforces the notion that edtech should be regarded as a tool within broader educational objectives. These objectives should prioritize and acknowledge the significance of social interactions and the role of teachers; aim to equip children with critical skills for navigating an increasingly digital world; and safeguard them from commercial influences that could compromise their well-being and infringe upon their human rights.

Chapter 10. The use of Google Workspace for Education in the European Union and in Brazil

834. Google Workspace for Education is widely used worldwide, but it impacts different communities in different ways. This chapter will focus on analyzing the impacts Google Workspace for Education has had on children's privacy and data protection in two different jurisdictions: the European Union and Brazil.

835. With regard to the EU, given the technology's extensive adoption and the controversies outlined in Chapter 9, it is not unexpected that complaints have been brought to the attention of competent authorities. The multiple analyses of the technology by public authorities in Europe provide important insights for this thesis. The publication of DPIAs in certain cases and the authorities' auditing capabilities allowed an in-depth analysis of the features of Google Workspace for Education. This level of scrutiny would be unattainable solely through the information publicly disclosed by the company.

836. This chapter will thus focus on discussing the decisions taken by authorities within the EU MS related to Google Workspace for Education. The methodology used to identify the decisions was twofold. First, I conducted searches for decisions regarding Google Workspace for Education within the databases of DPAs in Europe that are part of the EDPB. This encompassed not only the DPAs in each of the EU MS (and, in the case of Germany, in each of its *Länder*), but also those in the three countries that are part of the EEA: Iceland, Liechtenstein, and Norway. This search was supplemented by cross-referencing with the GDPR Hub and GDPR Enforcement Tracker websites. Second, the literature reviewed for this thesis also unveiled significant decisions regarding the use of the technology in certain countries and regions that were not covered in the initial search, such as the decisions taken by other authorities in France and Belgium. Ultimately, decisions relevant to the scope of this thesis were located in Belgium, Denmark, Finland, France, Germany, the Netherlands, Norway, Spain, and Sweden. Each of the subsections below will describe the violations of the rights to privacy and to the protection of personal data encountered by each authority and the implemented solutions.

837. When it comes to Brazil, however, there are still no decisions concerning Google Workspace for Education made by the ANPD. Due to the absence of this initial filter to map potential challenges to children's rights to privacy and data protection in the country, a different methodology was employed. In the Brazilian context, the standard documents used by Google

for the implementation of the application suite were scrutinized. This examination was supplemented by similar assessments performed by other researchers on prior versions of the relevant ToS and Privacy Policies, along with a broader analysis of the platform's deployment in Brazil and its procurement by Brazilian public authorities.

838. The subsequent sections will thus delineate the decisions made by authorities in each EU MS, as well as the challenges identified in the Brazilian case. A comprehensive analysis of the convergence or divergence in these decisions, as well as the interrelation of the realities of the two jurisdictions and the gaps still identified according to the normative framework, will be conducted in Chapter 11.

10.1 Belgium

839. The *Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens* (VTC - Flemish Supervisory Commission) was established on 25 May 2018 with the Belgian GDPR decree. It replaces the Flemish Supervisory Commission for Electronic Administrative Data Traffic that was instituted by the e-gov decree and has been operational since 2010, being responsible for supervising the application of the GDPR by the Flemish administrative authorities (VTC, [s. d.]).

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

841. In June 2021, the VTC published guidance on the procurement of software services and suppliers by public authorities in the Flemish region. It took note of the Flemish Government's

ambition to provide all pupils in the fifth and sixth years of primary education and the entire secondary education with an individual ICT device. However, it expressed concern about potential unintended side effects (VTC, 2021).

842. The authority highlighted that certain suppliers were unable to provide sufficient guarantees regarding the protection of children's data. This was particularly relevant for suppliers whose business model relied on the trading or commercial exploitation of personal data. Even if suppliers excluded the direct provision of advertising, there remained a risk that data could be used for other commercial purposes (VTC, 2021).

843. The VTC recommended that the government refrain from hastily purchasing such devices. It advised incorporating data protection criteria into the specifications of the public purchase, emphasizing adequate information security and limiting the use of data to the provision and organization of education. Furthermore, the VTC suggested selecting alternatives that offer the widest range of options for adjusting effective privacy settings effectively, ensuring that these settings are appropriately and thoroughly privacy-oriented. Finally, it urged the government to prepare the educational institutions that had already made investments in this regard for a transition aligned with these points of attention (VTC, 2021).

844. In June 2023, the VTC published a position on the use of Google Workspace for Education by primary and secondary schools in the Flemish region (VTC, 2023a). Referring to the previous guidelines mentioned above, it provided more details on this specific technology. The DPA highlighted the unequal relationship between Google and the individual schools and found it positive that the Department of Education and Training and the educational umbrella organizations have taken the initiative to enter into discussion with Google to negotiate better conditions for Flemish primary and secondary education, as happened in the Netherlands (which will be described in section 10.6). These Flemish authorities have then requested the VTC's opinion on the matter before agreeing to the proposal made by Google.

845. The VTC intended to first discuss Google Workspace for Education's privacy settings and, in a later consultation, the security vis-a-vis the supplier itself and third parties. Due to a Non-Disclosure Agreement, the authority had little knowledge about the actual terms of the agreement and had to seek information from Google itself, whose answer was considered not transparent enough (VTC, 2023a). Below are some highlights related to Google's answers and the respective comments issued by VTC (VTC, 2023a):

- i. The VTC found it concerning that ambiguities still existed regarding the roles and responsibilities of Google and schools within the GDPR. It should be evident when Google has any influence over the means and purposes of the data processing activities, potentially leading to its classification as a controller. The fact that this could change without schools' knowledge was also troubling, given Google's ability to unilaterally alter its ToS and Privacy policies. The VTC considered it unrealistic for schools to be regarded as controllers in certain data processing activities, taking into account the widely varying and sometimes limited expertise they have.
- ii. When schools are considered controllers, they are required to conduct DPIAs in accordance with art. 35 of the GDPR, concerning their intended use of Google Workspace for Education. The VTC also observed this requirement to be challenging and impractical, given that the majority of schools lack the necessary resources and expertise, as well as visibility into the risks dependent on Google's actions. Furthermore, conducting a DPIA does not guarantee that the essential technical and organizational measures, including the implementation of suitable privacy settings, have been effectively addressed.
- iii. Google stated that it would address the concerns of Flemish schools if they were similar to those of the Dutch public sector. The VTC noted that this assumption relies on schools being aware of the concerns of the Dutch public sector and that Google should bear the responsibility for developing appropriate solutions.

846. The authority highlighted that the solutions in the Netherlands are not guaranteed to be sufficient in the Flemish case (VTC, 2023a). It was of the opinion that the developments in the Netherlands case must be followed up and that similar concessions and guarantees must be obtained for Flemish education. Based on this, it advised that:

- i. Flemish schools using a limited number of Google applications should discontinue them unless adequate protective measures are taken, if at all possible.
- ii. For schools that have their ICT structurally embedded in Google, its use must cease by September 1, 2024, unless adequate protective measures are implemented, which should be at least equivalent to the safeguards negotiated

in the Netherlands. The VTC expects an exit plan to be drawn up in the meantime.

- iii. All schools using Google should be guided to achieve minimal data protection impact.
- iv. Switching to Google or new applications is not permissible until conclusive guarantees are provided that ensure effective management and protection of data in compliance with the data protection framework.
- v. Alternatives can be provided by the education umbrellas with support from the ministry.

10.2 Denmark

847. The Helsingør municipality in Denmark distributed Google Chromebooks installed with G-suite for education (now Google Workspace for Education) for its schools. While accessing YouTube with their school's accounts, students' full names, school, and class were displayed in their posts, unless aliases were used by the school, which prompted a complaint to the Danish DPA in December 2019. On 29 January 2020, Helsingør Municipality reported a personal data breach to the Danish DPA (Datatilsynet - Danish Data Protection Authority, 2021, 2022c). The Authority has also received other complaints related to this and other Municipalities, highlighting the absence of parental consent for the creation of the Google account and the parents' inability to correct or anonymize the information displayed while using it.

848. The Municipality argued that another legal basis was used rather than consent, i.e., the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. It also stated that it was not aware of the changes made in 2019 to Google's ToS, when several add-ons, including YouTube, were made available through the school account. In the Municipality's opinion, the information shared with YouTube was ordinary and Google had already access to it through G-Suite, which would not demand a DPIA (Datatilsynet - Danish Data Protection Authority, 2021).

849. The Danish DPA's September 2021 decision clarified that the Municipality could use art. 6(1)(e), GDPR, to justify the provision of Chromebooks and core Google Workspace for Education applications, as well as the processing activities related to the creation of the individual user. However, data disclosed to other controllers to be used for their own purposes,

such as the collection of metadata for marketing and profiling, would not be covered by the Municipality's exercise of authority (Datatilsynet - Danish Data Protection Authority, 2021).

850. The authority emphasized that the core services could have been configured in a way that: a) the processing activities do not exceed what is permissible under the Danish Primary and Lower Secondary Education Act; b) students' information would have been reduced to aliases; c) only the authorized profiles would be able to access data; d) data was not processed outside the EU/EEA (Datatilsynet - Danish Data Protection Authority, 2021).

851. Based on the above, the authority found that the Helsingør municipality has violated:

- a) Art. 4(12), GDPR, because in several cases students' full name were used, where an alias could have been applied instead;
- b) Art. 5(1)(a), due to the lack of lawfulness of the processing activity;
- b) Art. 5(1)(c), 5(1)(f) and 5(2), GDPR, because of the lack of documentation of the considerations of risks to data subjects' rights and the assessment of the processing carried out. Furthermore, it failed to demonstrate which system configuration was used and whether safety measures were ensured at that time of the data processing;
- c) Art. 32(1), by not having taken appropriate organizational and technical measures to ensure a level of security appropriate to the risks posed by the processing of data, especially within the context of additional services such as YouTube;
- d) Art. 33(1), GDPR, by not having notified the DPA within 72 hours after the municipality had become aware of the personal data breach;
- e) Art. 35(1), GDPR, because the use of new complex technology, especially in the field of education where children's data are processed, would entail a high risk to their rights and freedoms. This is particular pertinent when part of Google's business model is rooted in data collection and sale, as well as targeting advertisement.

852. The municipality was then ordered to bring the processing under compliance (Datatilsynet - Danish Data Protection Authority, 2021).

853. After assessing the new efforts and documentation provided by the municipality, the DPA found, in July 2022, that the processing of students' data did not meet the requirements of the GDPR and should be banned. Although Helsingør Municipality was considered to have done a significant and proficient job of mapping out how personal data is used in primary schools, the DPA highlighted how easy it is that data protection issues arise with the approaches

used by major tech companies (Datatilsynet - Danish Data Protection Authority, 2022c). The authority referred to its overarching work on the use of Chromebooks and Google Workspace for Education in Danish municipalities, indicating that this decision will probably likely extend to other municipalities using similar data processing structures.

854. In this second decision, the DPA found that the provided risk assessment generally addressed the most important scenarios and threats (Datatilsynet - Danish Data Protection Authority, 2022c). However, it failed to outline the risk scenarios stemming from the data processor design and the decisions made regarding the system. More specifically, this applies to the actual handling of personal data by the devices and applications, as well as to how Helsingør Municipality controls Google's access to personal data. This includes Google Chromebook's operating system and the interaction of Google Workspace with Google's backend concerning the necessary separation of personal data as mandated by the data processing agreement. This means that the Municipality has not demonstrated that personal data are processed lawfully, fairly and in a transparent manner in relation to the data subject.

855. In relation to the use of information for other purposes, the DPA emphasized that the Danish Primary and Lower Secondary Education Act establishes a list of lawful data processing activities, meaning that data must not be further processed. The Helsingør Municipality was only using Google Workspace for Education's core services and these do not process data for marketing purposes. However, the Municipality stated that a possible breach of the contractual obligations could not be ruled out, which would go against art. 28(1), GDPR, according to the DPA. The DPA was of the view that the data controller could only contract data processors who could guarantee their compliance with the data protection rules. Therefore, the mere expectation that it could breach the data processing agreement means that this data processor could not be selected by the controller (Datatilsynet - Danish Data Protection Authority, 2022c).

856. Although the Municipality framed this risk only as hypothetical, the DPA found that if it materialized, there would be a significant infringement upon the rights of the data subjects. No effective technical or organizational measures were documented to reduce this risk, and any risk involving high consequences for the rights and freedoms of data subjects, even when they are unlikely to be realized, should trigger the obligation to carry out a DPIA. The Municipality, therefore, also acted in breach of art. 35(1), GDPR (Datatilsynet - Danish Data Protection Authority, 2022c).

857. Regarding data transfer to third countries, the Municipality argued that, in general, data processed within Chromebooks and Google Workspace for Education would remain within EU data centers. However, there was still a risk that the support access was provided in third countries, which would demand a data transfer. The contract between the Municipality and Google included standard clauses pursuant to art. 46(2)(c), GDPR, as a basis for the transfer. However, the Danish DPA found that the transfer in question is covered by conditions in the USA that prevent the standard clauses from being a sufficient means of ensuring a level of protection that essentially corresponds to the level within the EU/EEA. Helsingør Municipality would be, thus, obliged to ensure that additional measures are put in place to bring the level of protection up to the required level.

858. According to the Helsingør Municipality, personal data was encrypted both in transit and at rest when the data were transmitted to and processed by Google, but Google would still be able to access the information in plain text, which does not guarantee sufficient protection. The DPA found, therefore, that the transfer does not occur in accordance with art. 44, GDPR, and that should be suspended until the Municipality demonstrates that provisions of Chapter V, GDPR, have been observed (Datatilsynet - Danish Data Protection Authority, 2022c).

859. After reviewing the material sent by the Municipality in early August 2022, the Danish DPA issued a new decision upholding the ban (Datatilsynet - Danish Data Protection Authority, 2022b). This time, the DPA prohibited Helsingør Municipality from processing personal data using Google Chromebooks and Workspace for Education.

860. A day after this decision, a meeting was held between the DPA, Helsingør Municipality, Local Government Denmark—the association and interest organization of the 98 Danish municipalities—and the Danish Agency for IT and Learning (Datatilsynet - Danish Data Protection Authority, 2022e). The meeting aimed to establish a shared understanding among the involved parties on how schools could legally use Chromebooks and Google Workspace for Education. In the meeting, Helsingør Municipality recognized the considerable risk associated with the data processing, and, as a result, all parties committed to quickly collaborate to bring the municipality's adoption of the technologies into compliance.

861. In September 2022, the Danish DPA lifted the ban but issued an order for compliance (Datatilsynet - Danish Data Protection Authority, 2022a). A similar injunction has been issued to Aarhus Municipality. This meant that students could resume using Google Workspace, but their permanent use would be subject to the handling of several issues related to contracts,

technology, and documentation by the Municipality. The DPA received additional material from the municipalities in November 2022 (Datatilsynet - Danish Data Protection Authority, 2022d), and, in December 2022, the association of the local governments—on behalf of the approx. 50 municipalities that use Google Workspace for Education—informed the DPA that they would submit further material in the case. Against this background, the DPA extended the documentation deadline to January 23, 2023, without issuing a new decision yet (Datatilsynet - Danish Data Protection Authority, 2022f).

10.3 Finland

862. In April 2018, the *Tietosuoja-valtuutettu* (Finish Data Protection Ombudsman) initiated an investigation related to the use of Google Suite for Education (now Google Workspace for Education) in a school within a municipality of Finland. More specifically, the DPA assessed (i) whether art. 6(1)(c) of the GDPR could be applied as a legal basis for processing personal data and (ii) whether the controller has appropriately ensured that international data transfers took place in accordance with data protection framework (Tietosuoja-valtuutettu, 2021).

863. In its statement, the controller specified that it processes students' data to comply with a statutory obligation, more specifically to provide basic education in accordance with the Finish Basic Education Act. The DPA was of the opinion that the law does not provide the specificities of the processing activities, and fulfilling this obligation as such would not require the use of digital technologies. The means of data processing are not defined by the law, and it leaves significant discretion to the controller in the processing of personal data (Tietosuoja-valtuutettu, 2021).

864. According to the authority, when the legal basis for processing personal data is compliance with a legal obligation, the law imposing it must fulfil all relevant conditions for the obligation to be valid and binding. It must also meet the requirements of data protection legislation, including necessity, proportionality, and purpose limitation and the controller must not have a choice as to whether or not it can comply with it. Therefore, voluntary unilateral commitments and public-private partnerships that process data beyond what is required by law would not fall within the scope of this legal basis (Tietosuoja-valtuutettu, 2021).

865. In this specific case, the DPA draws attention to the fact that digital technologies would process more data than traditional teaching activities. The DPA considers that, due to the various options available for providing education online, it would not be justified to

automatically consider the processing activities within this specific platform as necessary and proportionate. Instead, the controller should justify the processing of students' data on a case-by-case basis, according to its statutory obligation to provide basic education (Tietosuojavaltuutettu, 2021).

866. When assessing other possible legal bases for processing students' data by the municipality, the DPA considered that consent cannot be freely given if the data subject does not have a genuine free choice and cannot refuse or withdraw consent without detriment. This does not imply that it should be outrightly disregarded in instances where there is a power imbalance between the controller and the data subject. However, the controller would need to demonstrate the voluntary nature of consent and ensure that data subjects who refuse to provide their consent are offered a genuine, equal alternative (Tietosuojavaltuutettu, 2021).

867. Apart from the analysis regarding the legal basis, the authority highlighted that by accepting the standard ToS offered by Google, the controller has affected its ability to properly control and supervise the processing of personal data. The DPIA carried out by the controller itself recognizes the risks arising from the general terms and conditions. According to the municipality, since the terms and conditions are general and partly difficult to interpret, there is a risk that the processing activities are not defined in a sufficiently transparent and clear manner. The ombudsman also notes that the technology is not only used within the school but also in students' homes and own devices, which would require the data processing activity to be voluntary in these cases (Tietosuojavaltuutettu, 2021).

868. According to the DPA, due to its obligations related to data protection by design and by default, the controller must assess all functionalities of a service, especially when it is provided for free. It should pay attention to the type of service entity, how the controller is determined when using different parts of the service package, and which contract terms will be applied at any given time. Finally, the controller also failed to implement encryption, as the method used is considered outdated in terms of data security (Tietosuojavaltuutettu, 2021).

869. When it comes to data transfers to third countries, considering the existence of personal data transfers from the EU to the USA and the Schrems II ruling. The DPA requested information from the controller on whether it has introduced additional safeguards after the annulment of the Privacy Shield, which was not confirmed.

870. Based on the above, the DPA considered that art. 6(1)(c) of the GDPR does not apply to the processing of personal data, which means that the processing activities violated the

GDPR. The controller was reprimanded and ordered to bring processing operations into compliance. Regarding the international data transfers, the Municipality was ordered to notify the DPA of the measures it has taken as a result of the EDPS guidance on the matter (Tietosuojavaltuutettu, 2021).

10.4 France

871. In August 2022, a member of the French National Assembly, Mr. Philippe Latombe, raised concerns with the French Minister of National Education and Youth regarding the use of Microsoft Office 365 in schools. He emphasized that while free services might appear attractive, they pose risks to competition and data sovereignty (Assemblée Nationale, 2022b, p. 3866).

872. In his written response, the French Minister explained that, according to the French Public Procurement Code, public procurement contracts are typically intended for pecuniary interest to meet specific needs of public entities in terms of works, supplies, or services. Therefore, free offers of services would be, in principle, excluded from the scope of public procurement (Assemblée Nationale, 2022b, p. 3866). The Minister acknowledged that providing schools with a free office suite is probably meant to familiarize the public with the tools, increasing the likelihood of them later subscribing to the paid version. However, he considered that this indirect benefit does not make the service onerous in itself (Assemblée Nationale, 2022a).

873. The Minister also referred to several documents and recommendations: a) the Prime Minister's Circular No. 6282-SG on the Cloud at the Center Doctrine; b) a note from the Interministerial Director of Digital Affairs (*Directeur Interministériel du Numérique* - DINUM) dated September 15, 2021, indicating that Microsoft Office 365 did not comply with the Doctrine; and c) a letter from the Commission Nationale de l'Informatique et des Libertés (CNIL) dated May 27, 2021 (Commission Nationale de l'Informatique et des Libertés (CNIL), 2021), recommending that higher education institutions use collaborative suites offered by providers subject to European law, which host the data within the EU and do not transfer them to the USA. The Minister added that this also applied to Google Workspace for Education.

874. The Cloud at the Center Doctrine, adopted by the French Government, highlights that the cloud has become the default mode of hosting and producing the state's digital services. It aims at meeting French people's legitimate expectations of an exemplary state in terms of

protecting their data and guaranteeing the continuity of the public service, two prerequisites for their confidence in the digital public service. The digital services offered by the administrations must then be hosted on one of the two internal interministerial clouds of the state or on Cloud offers of manufacturers that meet strict security criteria (Borne, 2023; DINUM, [s. d.]).

10.5 Germany

875. In August 2018, Microsoft announced the end of its collaboration with Deutsche Telekom in providing Microsoft cloud services, including Office365, under strict German jurisdiction (the so-called German Cloud) (Dedezade, 2018). Under this agreement, data was handled by a trustee under German rules and Microsoft employees had no access to them (Poortvliet, 2018). After this decision and having received several complaints from teachers and school administrators, in July 2019 the German Land of Hesse's DPA prohibited the use of Microsoft Office 365 in schools since children's data were being stored in a European Cloud. The same decision was also extended to Google and Apple services using a similar cloud.

876. The rationale was based on several arguments. First, with the by then newly enacted USA Cloud Act, USA government agencies could request access to customer data from all USA-based companies even when the servers were outside the USA's territory. Second, it stressed the responsibility of German public institutions regarding data processing legality and traceability (Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 2019a). The decision also mentioned the need for guaranteeing the state's digital sovereignty; and the unclear nature of telemetry data transmitted to Microsoft (Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 2019a). Concerns that Windows 10 and 11 operating systems collect telemetry data had already been expressed by the Germany's Federal Office for Information (BSI, in German) (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018). Finally, the DPA stressed that gathering parent's consent would not be a solution to the issue, as the security and traceability of the data processing were not guaranteed.

877. A month later, however, the ban was lifted by the Supervisory Authority, which decided to "temporarily tolerate" the use of Office 365 in Hessian schools under certain conditions and subject to further examination (Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 2019b). This happened after negotiations with Microsoft and a change in the DPA's assessment, which refuted some of the concerns. One of the applied safeguards was

preventing the transmission of any kind of diagnostic data. Google and Apple services were not mentioned in this second decision.

878. Specifically regarding Microsoft Office 365, it also faced bans in 2020 by the State Commissioner for Data Protection and Freedom of Information Baden-Württemberg (Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, 2022), as well as in 2022 by North Rhine-Westphalia Data Protection Authority (Brinkmeyer, 2023; Gayk, 2023). This decision was confirmed in 2021 (Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, 2021). In November 2022, the German Data Protection Conference (DSK, in German)—the committee of Independent German Federal and State Data Protection Supervisory Authorities—published a the report of the DSK working group on Microsoft 365, concluding that the software still did not comply with the GDPR (Datenschutzkonferenz, 2022). The extension or applicability of this decision to other similar technologies, such as Google Workspace for Education, is still not confirmed.

879. The use of Google Services was also prohibited at one of Dortmund's seven secondary schools, after a student's privacy concerns led to his refusal to use the platform in 2021. Despite the school offering an alternative solution, it was rejected as it was believed that participating in school activities without discrimination was not possible. Unable to use the same tools as their peers, the student could not engage in visual exchanges with teachers, submit his/her homework, and upload solutions, as the communication was only done via email. The student eventually filed a complaint with the Petitions Committee of the State Parliament, and, after some appeals, the case reached the Higher Administrative Court of North Rhine-Westphalia (mrtee, 2023a).

880. Google Workspace for Education has been procured by the school itself but the latter was unable to prove the data protection conformity of the platform. Following the discussions, the judge presented a proposal to the representatives of the Arnsberg district government, which would ensure that Google Workspace for Education would no longer be adopted and students would use a platform whose compatibility with national and European data protection law has been checked (mrtee, 2023a). The Arnsberg district accepted the proposal and the school announced on its website that it has been instructed to discontinue the use of Google Workspace for Education after Easter Holidays 2023 (mrtee, 2023b).

10.6 Netherlands

881. In February 2021, SURF—the collaborative organization for IT in Dutch education and research (SURF, [s. d.])—and SIVON—a cooperative of school boards in primary and secondary education (SIVON, [s. d.])—disclosed that a DPIA of Google Workspace for Education had been commissioned by the University of Groningen and Amsterdam University of Applied Sciences (SURF, 2021c).

882. Completed on 15 July 2020, the DPIA identified ten high²⁹ and three low³⁰ data protection risks affecting data subjects when they used Google Workspace for Education (Nas, Sjoera; Terra, 2021). More specifically, it found that Google could not qualify as a data processor for the collected personal data, and, as joint controllers, Google and the universities lacked legal grounds for their processing activities. According to surveys conducted by SURF and SIVON, Google Workspace was employed by 52% of primary schools and 36% of secondary schools in the Netherlands. It was also used by certain faculties within 4 out of the 14 universities and 4 out of the 36 government-funded universities of applied sciences across the country (Nas, 2021).

883. After providing the first version of the DPIA to Google, discussions took place until January 2021, during which Google implemented various technical and organizational measures to mitigate risks, particularly regarding consumer data (Bonamigo, 2021). For example, measures were taken to prevent spill-over of personal data, such as when end-users access additional services with their Google Account, as well as to address privacy-unfriendly default settings (Nas, Sjoera; Terra, 2021). However, only these two of the ten high risks had been completely mitigated.

884. Due to the remaining risks identified by the DPIA, SURF and SIVON asked for advice from the Dutch Personal Data Authority (Autoriteit Persoonsgegevens, AP). Based on the documentation provided by the two institutions, the AP advised them (and therefore the educational institutions they represented) not to start or continue using Google Workspace for

²⁹ The ten high data protection risks identified by Privacy Company were: Lack of purpose limitation (in relation to customer data); lack of purpose limitation (in relation to diagnostic data); lack of transparency (in relation to customer data); lack of transparency (in relation to diagnostic data); lack of lawful grounds for processing personal data; missing privacy controls; privacy-unfriendly default settings; the use of multiple Google accounts; lack of control of subprocessors; lack of access by data subjects to their personal data.

³⁰ The three low data protection risks identified by Privacy Company were: Unlawful access to customer data and diagnostic data in the USA by the cloud provider; the chilling effect generated by the employee monitoring system; and the impossibility of deleting individual diagnostic data.

Education before the problems raised were solved (AP, 2021a). More specifically, the authority advised them to determine a) which processing of personal data takes place and for which purposes; b) which parties determine the purpose and (essential) means of the processing activities and the roles they assume as a result; c) the lawful bases for the intended processing activities; and d) the specific risks related to the processing of children's data, insofar as applicable for the relevant educational institution(s). In the same document, the AP warned that if SURF and SIVON could not reach an agreement to sufficiently mitigate the risks related to Google Workspace for Education, it should be phased out before the start of the 2021/2022 school year.

885. The AP also addressed two letters to the Dutch Minister for Primary and Secondary Education, and Media, and to the Dutch Minister of Education, Culture, and Science (AP, 2021c, 2021b). They were advised to coordinate efforts, including within the EU with other MS; inform educational institutions about their responsibilities; explore which digital resources are commonly used by educational institutions; and having them carry out DPIAs. Furthermore, specific actions related to Google Workspace for Education should be taken, such as communicating the outcomes of the advice to educational institutions, mapping which of them used the software, and investigating the possibilities for educational institutions to take measures independently to reduce risks. In a letter sent to the House of Representatives in June 2021, the Ministry of Education, Culture and Science said it expected Google to resolve the identified issues before the start of the 2021/2022 school year (Ministry of Education, 2021).

886. In July 2021, Google and the educational institutions reached an agreement to sufficiently mitigate all high risks identified in the DPIA (SURF, 2021a). These measures mostly applied to Google Workspace for Education's core services, but Google has committed itself to continue discussions with SURF and SIVON to solve issues related to the Google Cloud Platform and Chrome OS (the operating system for the Chromebooks) (SURF, 2021a). This meant that the education institutions could resume Google Workspace for Education use, provided that specific measures were applied (SURF, 2021b).

887. A new DPIA report was then requested by SURF and SIVON to Privacy Company, which was published in August 2021. The report shows that Google had finally agreed to lower the eight remaining high data protection risks (Nas, Sjoera; Terra, 2021). For instance, Google has agreed to act as a data processor for the Diagnostic Data about the individual use of the services; to implement measures to increase transparency; and to develop a processor-version of the Chromebooks and the Chrome browser (Nas, 2021). Google remained as a data controller

for additional services and would not provide additional safeguards in relation to them. In this case, students would need to use them with a personal account.

888. The new DPIA also directly addressed children's data processing and consent for additional services, which was previously omitted. Privacy Company explained that Google was found to be a data controller for the additional services. If they were used in schools, consent from end-users would need to be obtained. However, there was clearly an imbalance of power between schools and parents/children, as they are frequently not in a position to refuse the service, and their consent would most probably not be valid (Nas, Sjoera; Terra, 2021).

889. Before September 2021, Google would automatically log students out of their school accounts when they accessed additional services, and their data would be anonymized. However, Google has discontinued this option. When using YouTube, for instance, students were limited to viewing content without the option for anonymous interaction. Additionally, even though they were not subjected to personalized advertisements, students were still exposed to contextual ones. Consequently, the DPIA anticipated that the only viable course of action would be for schools to disable these additional services. When teachers desire to use any YouTube video, for example, they should embed them within Google Classroom (Nas, Sjoera; Terra, 2021). It should be noted, however, that the risk of creating personal accounts should also be considered by schools. Although they can technically prevent access to additional services at the school environment, as well as simultaneous log-in, they would not be able to prevent students from creating a personal account (Nas, Sjoera; Terra, 2021).

890. The agreement was said to prompt global changes in Google Workspace for Education data processing (Crandall, 2022b), which as we saw in the Belgian case (and will see in the Brazilian case), was not actually the case. Considering that some schools might need to carry out DPIAs for their specific cases, Google also created a Cloud DPIA Resource Center (Crandall, 2022a; Google, 2023d).

891. In December 2022, SIVON and SURF reported Google's progress in addressing the risks identified in the 2021 DPIA, with ongoing efforts to solve remaining issues by mid-June 2023 (SURF, 2023b). Despite negotiations, the DPA was still concerned about the Minister's additional findings, especially if any substantial privacy risks for students remained. On 8 March 2023, the AP issued a letter to the Dutch Government asking for urgent clarifications regarding the possibility of using Google Workspace for Education in schools in a lawful manner before the beginning of the 2023-2024 academic year (AP, 2023).

892. On 20 April 2023, the Ministry of Education, Culture, and Science informed the House of Representatives how the advice from the DPA was followed (Ministerie van Onderwijs, 2023). It explained the agreements made between SIVON, SURF, and Google and the fact that schools would receive instructions about Workspace for Education by mid-June 2023 (SIVON, 2023). A verification report was issued by Privacy Company confirming the measures implemented by Google (Nas; Terra, 2023). However, the new assessment revealed new potential risks, which were meant to be discussed separately between SURF, SIVON, and Google.

893. Regarding the separate negotiations on the ToS governing the utilization of Chrome OS and the Chrome browser on Chromebooks, SURF and SIVON reached another agreement with Google in May 2023. Under these revised ToS, Google would be a data processor in relation to “essential services” (SURF, [s. d.]), while additional services would need to be turned off by the administrator (SURF, 2023c). The new processor version would become available in August 2023. Additional agreements were made to eliminate other privacy risks (SURF; SIVON, 2023), and an inspection report was published (Terra *et al.*, 2023). This allowed SURF and SIVON to conclude that Dutch educational institutions could continue to use Google Workspace for Education and Google Chromebooks (SURF, 2023a).

894. Finally, it is important to mention that a separate process started in the beginning of 2023 to address concerns pertaining to data transfers, particularly to the USA. A Data Transfer Impact Assessment (DTIA) was underway and was anticipated to conclude in autumn 2023 (SURF, 2023a).

10.7 Norway

895. Although not part of the EU, Norway is part of the EEA and adopts the GDPR. As per the Decision n. 154, of the EEA Joint Committee, the EEA countries not part of the EU are also members of the EDPB, although without voting rights and the right to be elected as chair and vice-chair. Therefore, the decisions taken by the Norwegian DPA, Datatilsynet, are also relevant for this part of the thesis, where the violations of the GDPR are analyzed.

896. In Norway, several municipalities have adopted Google Workspace for Education in primary and lower secondary schools. Based on some parents’ complaints coming from parents, the DPA has taken a closer look at three of them (Datatilsynet - Norwegian Data Protection Authority, 2020b).

897. Although based on different complaints and different grounds, the decision taken in relation to these three municipalities were focused on the same four issues identified by the authority: (i) the municipalities have not kept a log of processing activities taking place on students' Chromebooks and in G Suite for Education; (ii) they have not implemented appropriate technical and organizational measures to achieve a level of security appropriate to the risk; (iii) they have not conducted a privacy impact assessment of the use of Chromebooks and G Suite for Education in schools; and (iv) they have not provided adequate information to enable students and parents to safeguard their interests and privacy when using Chromebook and G Suite for Education (Datatilsynet - Norwegian Data Protection Authority, 2020e, 2020c, 2020d).

898. With respect to maintaining a record of processing activities, Sandnes municipality has stated that no protocol has been created for processing activities related to the use of Google Chromebook and G Suite for Education. In Strand municipality, a protocol has been created, but upon revision of the DPA, several shortcomings have been identified, such as the legal basis used for processing students' data. Although the municipality would rely on the performance of a contract and consent, the DPA was of the opinion that the processing was necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The same issue was detected in the Bergen municipality case. While the municipality considered that a legal obligation would be the appropriate legal basis, the DPA recommended using art. 6(1)(e) instead. In the Bergen municipality case, the DPA also found that the purposes for data processing were not specific enough.

899. The DPA also stated that when acquiring hardware and software to be used in schools, municipalities must carry out a risk assessment based on art. 32, GDPR, to analyze the security of the processing. This was not conducted by Sandnes municipality. Strand and Bergen municipalities have provided a risk assessment to the DPA, but the latter considered that they have not implemented sufficient measures to keep themselves informed of future changes to Google's ToS, which would result in more risks to students.

900. With regard to the assessment of data protection risks, the DPA was of the opinion that a DPIA was mandatory in the case of implementation of the platform by the municipalities. These processing activities would meet at least two criteria present in the DPA's guidance on DPIAs: the involvement of vulnerable subjects and the innovative use or application of a new technological or organizational solution (in this case, the use of cloud services in primary schools).

901. Finally, concerning the provision of sufficient information to data subjects in accordance with arts. 12 through 14 of the GDPR, the DPA held the view that municipalities have fallen short. Sandnes municipality asserts that this obligation was met by conducting a meeting with the children's parents, who then signed a form at its conclusion. However, this information was not supplemented by any information in writing, and parents were given only a few minutes after the presentation to sign the form. A similar situation occurred in Strand municipality. In the case of Bergen municipality, although the controller mentioned a meeting had taken place, the complainants argue that the information was rather provided in a fragmented way, which they considered insufficient.

902. The DPA found that the information given to parents was not enough to meet the GDPR requirements, especially because the service was targeted to children. Simply referring to Google's ToS was not considered enough. The DPA also mentioned the need for schools to provide clear information about where their responsibility stops and the parents' responsibility begins. If it is the case that the children can use the Chromebook for private purposes, and log in with private accounts through the browser, the municipality should clearly inform about the privacy risks that may arise from private use.

903. After dealing with these three cases, the DPA issued guidelines applicable to all municipalities within Norway mainly focused on Google Chromebooks and Google Workspace for Education, but also very much transferable to other cloud services (Datatilsynet - Norwegian Data Protection Authority, 2020a).

10.8 Spain

904. In the case of Spain, two decisions are important for the scope of this thesis. The first decision originated from a complaint of a parent, dated July 2021, who argued that they were not consulted for the implementation of G Suite for Education (now Google Workspace for Education) in a school under the organization of the Consejería de Educación, Universidades, Cultura y Deportes del Gobierno de Canarias. According to the Spanish DPA, Agencia Española de Protección de Datos (AEPD), the now Google Workspace for Education gained prominence with the onset of the COVID-19 pandemic as a digital tool in Spanish schools due to the absence or insufficient resources available to them (AEPD, 2023a).

905. The first data protection issue identified by the DPA in this case was the lack of proper information provided to the data subjects as per art. 13, GDPR. The authority listed several

elements that were missing from the documents provided by the school to parents and students. It considered this particularly concerning because consent served as a legal basis for processing students' data and, in certain situations, students themselves would provide consent if they were aged 14 or older. The DPA considered that the language of the documents was not clear and simple so a minor could understand. This issue has, therefore, led to the lack of a proper legal basis for processing personal data, which would also infringe art. 6(1), GDPR (AEPD, 2023a).

906. The second element identified by the DPA was the incompleteness of the DPIA carried out by the controller. The controller used a template provided by the authority to identify the risks associated with the platform. However, it failed to identify specific risks related to Google Workspace for Education, which would prevent it to take adequate measures to address them, especially due to the involvement of minors. The DPA also considered that the controller's conclusions reached within the DPIA were not well-founded and logical in relation to the facts (AEPD, 2023a).

907. The second relevant decision of the AEPD is related to the use of Google Workspace for Education at Colegio Menor Nuestra Señora de Loreto. It also originated from a parent's complaint dated August 2021, who argued that consent had not been provided for the use of the tool within the school. The authority clarified that, in this specific case, the school would not need to request parents' consent, as it cannot be considered an adequate legal basis due to the power imbalance between the controller and the data subject. The appropriate legal basis in this case would thus be art. 6(1)(e) (AEPD, 2023b). This is an interesting conclusion, as in the previous case the authority has not questioned consent as an appropriate legal basis, just the appropriateness of the information received by the parents and data subjects.

908. Despite the legal basis not being deemed inappropriate, other issues were identified by the authority. The use of Google Workspace for Education in this specific school was implemented based on Google's ToS. The DPA considered that this agreement was not enough to clarify the roles and responsibilities between the controller (the school) and the processor (Google), as well as to implement the requirements of art. 28, GDPR (AEPD, 2023b).

909. A second issue identified by the authority was the lack of proper information related to the processing activities provided to the data subjects, which would be in breach of art. 13, GDPR. The DPA considered that the information given to parents and students was not presented in simple, intelligible, concise, and didactic language for easy understanding (AEPD, 2023b).

910. It is important to mention that there was an appeal to this decision from August 2023. The decision regarding the appeal was published in November 2023. The DPA considered that the appellant did not present new facts or legal arguments that would allow reconsideration of the validity of the challenged decision (AEPD, 2023c).

10.9 Sweden

911. The Swedish Authority for Privacy Protection (Integritetsskyddsmyndigheten - IMY) initiated a procedure to investigate whether the barn- och utbildningsnämnden (Children and Education Board), in Östersund Municipality, has failed in its obligation to conduct an impact assessment before the introduction of Google Workspace for Education in 24 schools in the fall of 2020 (IMY, 2023a).

912. In a response to IMY, the board stated that the Jämtland County Regional Council conducted a risk analysis of Google Apps for Education (now Google Workspace for Education) in 2014. The analysis showed that there were no significant risks in relation to the use of the service. In May 2020, the council decided to move the service to its own domain, and by June 2020, the service was active in the council's IT environment. However, after the migration, the Board identified shortcomings in managing the new domain (IMY, 2023a).

913. Although the migration assessment resulted in the same risks as the 2014 analysis, documentation was not prepared in accordance with applicable legislation, considering the relocation of the service to a separate domain. The board has initiated training for IT administrators to ensure that they can manage the service according to the instructions provided by the board. The next step involved conducting an audit, which was included in the consultation of the impact assessment. Since the audit has not been finalized, neither has the impact assessment. The latter would also include an analysis of whether the use of the service involves transferring personal data to a third country (IMY, 2023a).

914. In the decision, the DPA considered that the Board is the data controller for the processing of personal data when the service is used in the municipality's schools. It also provides examples of how the service is used and the types of data that are collected. The service is employed by schools, for instance, for teaching and communication, distributing planning and assignments to students, providing feedback to students, and facilitating communication between students when needed for specific assignments, etc. Examples of the data collected include first name, last name, email address, class, and group membership. Based on the data

collected in other cases described in this thesis, it seems likely that these are only the data directly provided by the school, and not data collected by Google itself to provide the services.

915. In September 2023, a communication from the Board to the DPA outlined the outcomes of an audit, which unveiled several risks that demanded further work to identify solutions. However, the safety deficiencies had been effectively addressed, with numerous safeguards already implemented. For instance, the Board signed an agreement with Google for an extended license, ensuring data encryption and facilitating the implementation of security protocols mandated by the audit within the municipality's IT infrastructure. Furthermore, the municipality has implemented policy documents, training programs, information management plans and restrictions on the storage/processing of personal data (IMY, 2023a).

916. The IMY observed that the processing activities involved 5,945 children within the context of education, wherein the data subjects are highly dependable on the controller. The large-scale processing and handling of data from vulnerable individuals already satisfied two criteria from the list developed by the authority based on art. 35(4) of the GDPR. Moreover, the impact assessment has not been completed even after three years of the beginning of the processing activities, indicating a high degree of negligence. Consequently, on November 30, 2023, the IMY imposed an administrative fine of SEK 300,000 (approximately 26 thousand euros) against the board of Östersund Municipality (IMY, 2023b). It is important to mention that this was the only situation of the cases analyzed in the thesis where there a fine was issued.

10.10 Brazil

917. The Brazilian Internet Steering Committee, through its Network Information Center, conducts an annual survey on the use of the internet and digital resources in Brazil. One of its surveys focuses on the use of ICT in education, which serves as a crucial and reliable source for understanding the Brazilian context where Google Workspace for Education is deployed.

918. The data for the 13th edition of the survey was gathered between May 2022 and October 2023, marking the first in-person data collection following the reopening of schools after the COVID-19 pandemic. Through the historical series of the survey, it is possible to identify an increase in the connectivity of Brazilian schools. According to the latest findings, 93% of public primary and secondary schools, and 99% of private schools now have access to the internet (Brazilian Network Information Center, 2023).

919. However, apart from universal connectivity (connectivity for all), it is also important to provide meaningful connectivity (“a level of connectivity that allows users to have a safe, satisfying, enriching and productive online experience at an affordable cost” (International Telecommunication Union (ITU), 2022, p. 2). The survey found, for example, that in municipal schools it is common for the internet connection not to support multiple simultaneous access (45%). Other issues such as a poor signal range within the school premises (38%), poor internet quality (35%), and frequent internet crashes (34%) were also identified (Brazilian Network Information Center, 2023).

920. In relation to the use of digital devices, mobile phones were the most popular among teachers (67%), while computers (53%) and tablets (14%) were mentioned less frequently. Among all teachers, 31% used their personal devices and 24% used school devices. 8% mentioned that mobile phones were the exclusive means for accessing the internet with their students. Within their households, 42% of students had portable computers, followed by desktop computers (31%) and tablets (26%). 83% of the students had a mobile phone of their own that could be used for educational activities (Brazilian Network Information Center, 2023).

921. When it comes to digital applications and platforms used within schools, 77% of them employed online class record books or student enrollment, grade, and attendance control systems. In the 2022 edition of the survey, 33% of the schools said they officially adopted a LMS, compared to 51% in the 2020 edition, most probably attributed to the return to in-person classrooms. Nevertheless, 47% of the teachers reported using a LMS and 48% reported using Google Classroom, indicating a misunderstanding of what is meant by a LMS (Brazilian Network Information Center, 2023).

922. Among the criteria used to choose an edtech, being free appeared as the primary factor for 69% of educators, surpassing even its suitability to the curriculum and learning objectives. The survey highlights, however, that data protection has also been a concern among educators. For instance, 27% of primary and secondary education schools have refrained from adopting an edtech due to these concerns (Brazilian Network Information Center, 2023).

923. Another significant endeavor mapping the Brazilian reality is conducted by the *Observatório Educação Viglada* (Surveilled Education Observatory). Led by academic researchers and NGOs, this initiative is dedicated to collecting and disseminating information concerning the integration of platforms in public education across Brazil and South America (Observatório Educação Viglada, [s. d.]). To map the presence of large technology companies

in Brazilian education, the project has developed software capable of identifying the storage location of official email servers used by public educational institutions. The results underwent a qualitative validation process through freedom of information requests.

924. According to the latest data, 51.22% of Brazilian state schools incorporate Google services in their educational systems, while 24.39% rely on Microsoft. Of the 52 municipal schools across Brazilian cities with populations exceeding 100,000, 14 use Google services, 10 use Microsoft, and 32 employ other services. Notably, 4 of these schools use both Google and Microsoft services simultaneously (Amiel *et al.*, 2021). Another research based on freedom of information requests made to the Education Secretariats of the Brazilian Central Government, the Federal District, and the states of Amazonas, Maranhão, Rio de Janeiro, and São Paulo, confirmed that all of them used Google Workspace for Education (Núcleo de Informação e Coordenação do Ponto BR, 2022).

925. The increasing use of private platforms within education is directly linked to the lack of public investment in education, especially in ICT (Cruz; Venturini, 2020). Apart from economic crises and neoliberal policies, the COVID-19 pandemic created the need for a sudden adoption of technologies without a proper public debate on how this should be done. It caught governments off guard, as they were mostly not technically and organizationally prepared for the implementation of technologies supporting distance education overnight. The urgency in the decision-making and the lack of a holistic view of children's fundamental rights often led to the implementation and, to this day, the maintenance of problematic edtech. Before the pandemic, only 21% of Brazilian schools provided remote learning activities and the use of LMS grew dramatically between 2019 (28%) and 2020 (66%) (Brazilian Network Information Center, 2021)

10.10.1 The formalization of the relationship between Google and the schools

926. Having mapped all the partnerships carried out by Google and State Education Secretariats in Brazil until 2023, Lopes (2023) identified that the state of Minas Gerais was the first to establish an agreement for the provision of Google Apps for Education in 2009. Since then, out of the 27 Brazilian federative units, direct partnerships were not identified in only 4 of them.

927. In 2018, in collaboration with the Lemann Foundation, Google was already directly influencing the content taught in Brazilian schools. Within the NOVA ESCOLA policy, for

example, the organizations launched the first templates of digital lesson plans aligned with the National Common Curricular Base (BNCC)³¹.

928. In 2019, the National Council of State Secretaries of Education (*Conselho Nacional de Secretários da Educação - Consed*)³² was approached by Google to establish a partnership for the provision of Google Workspace for Education to the networks of state schools whose secretaries were signatories to the agreement. Despite this partnership, many states signed new agreements after 2020 due to COVID-19 in order to extend the duration of the partnership or include addendum terms (Lopes, 2023).

929. In 2022, the Brazilian Ministry of Education itself signed a partnership with Google for the implementation of Google Workspace for Education in federal educational institutions and making it available for other federative entities throughout the country (Nascimento, 2022).

930. Legal arrangements between schools and Google vary across the Brazilian educational landscape. In a study conducted by Amiel *et al.* (2021), which involved information requests to public educational institutions including State Education Secretariats, Federal Institutes of Education, and Federal Universities, diverse modes of adherence to Google and Microsoft technologies were observed. These include terms of cooperation, agreements, work plans, etc. In some situations, the object of the agreements is shaped to specify a mere technical consultancy service using expressions such as “encouraging the adoption of technology,” “providing solutions,” “promoting the improvement of educational actions,” and “creating an environment” (Núcleo de Informação e Coordenação do Ponto BR, 2022).

931. This legal relationship is frequently established directly through Google’s website, where schools accept its ToS and other policies. This contradicts the response to some information requests received by the researchers, which state that the school had no contract with Google, despite confirming its use. The ease of access to the services can lead to the erroneous conclusion that there is no legal relationship involved, particularly because it is perceived as a “free” service (Amiel *et al.*, 2021). Even in cases where the school does not use the technology, this does not imply a lack of ties with Google. On the contrary, one of the strategies used by the company is to directly contact teachers, laboratories, etc., which

³¹ The BNCC is a public policy endorsed in 2017 that defines what each student is entitled to learn in school and directly impacts classrooms across the country (Consed, 2018).

³² The National Council of State Secretaries of Education is an association founded in 1986, which brings together the Secretaries of Education from the States and the Federal District. Among its purposes are the integration of state education networks and the participation of states in the development of national policies, as well as collaboration among the federative units (Consed, [s. d.]).

facilitates the use of technology and circumvents the basic bureaucratic hurdles for its use by the school.

932. Partnerships between the schools and Google could also be formalized through intermediaries such as local start-ups that would embed Google Classroom in their apps (Derechos Digitales; Privacy International, 2022). Other type of intermediaries include foundations and other companies that fund a specific project where the app is used (Núcleo de Informação e Coordenação do Ponto BR, 2022).

933. In 2018 and 2019, Google conducted several presentations nationwide to showcase the company's applications, which included Google Workspace for Education, and to train professionals in their use (Leme, 2019). This is facilitated by the great amount of autonomy that states and municipalities have within the Brazilian legal framework.

934. Although the focus of this research does not revolve around public procurement rules, it is important to note that, according to Brazilian Law, cooperation terms should be used only when both parties share a common interest (aligned with the public interest) and no transfer of resources is permitted. These are instruments outlined in Law n. 13,019 (Brasil, 2014) and meant for establishing partnerships between the administration and civil society organizations. Although the law itself does not explicitly mention for-profit entities, the majority of Brazilian legal scholars argue that, considering the company's social function and the principle of solidarity, it would still be possible to establish partnerships not involving the transfer of funds between the state and for-profit entities, thus bypassing bidding laws.

935. The absence of monetary transfer, as previously explained, does not imply that the product can be considered free or that there is no economic interest on the part of the company in the contract. The existence of common interests, particularly aligned with the public interest, is also questionable. This is particularly serious when contracts are mostly standardized and easily signed over the internet.

936. Consequently, important steps that guarantee transparency and due process within bidding procedures are not followed. Art. 118, of Law n. 14.133, 2021, states that the provisions within this law could govern this type of agreement, where applicable, in the absence of a specific regulation. Thus, although cooperation agreements are *a priori* exempt from the specific rules of the bidding process, they are not entirely outside the scope of application of Law no. 14,133. In the absence of specific legislation for similar instruments, there is subsidiary

application of the legislation and, in particular, the dimension of constitutional principles of administrative law (Núcleo de Informação e Coordenação do Ponto BR, 2022).

937. This does not reflect the current Brazilian context, though. Other factors that should influence the procurement beyond the price of the product or service, such as the degree of protection of children's fundamental rights, are also not taken into account, as demonstrated by research conducted by Derechos Digitales and Privacy International (2022), as well as the data from Brazilian Network Information Center, mentioned above (2023). Cruz and Venturini (2020) also emphasize that some educational departments adopted Google's technologies because they were already used by teachers and students, making the transition to a remote/hybrid learning environment smoother. Another study shows that certain states adopted the technology based on its approval by other states in the country, indicating it had undergone some kind of vetting and testing (Núcleo de Informação e Coordenação do Ponto BR, 2022). Therefore, there is a real lack of acceptable grounds that justify the procurement of this technology in particular, beyond mere convenience and its free-of-charge nature.

10.10.2 Privacy and data protection issues

938. In order to use Google Workspace for Education, Brazilian schools must comply with various documents provided by Google. The Google Workspace for Education ToS (Google, 2023f) serves as the main contract between the parties, in the absence of a specific offline version. In addition, the use of the products is also governed by the general Google ToS (Google, 2022), the Google Cloud ToS (Google, 2023e), the Google Workspace for Education Privacy Notice (Google, 2023b), the Google's general Privacy Policy (Google, 2023d), the Google Cloud Privacy Notice (Google, 2023a), and the Cloud Data Processing Addendum (Customers) (Google, 2023c).

939. The Google Workspace for Education Privacy Notice is the primary governing document for the application suite and should take precedence in the event of any conflicting clauses with other notices. Within this document, Google delineates the distinction between core services and additional services already mentioned above to elucidate the implications each one has on the personal data of users. In the sections below I will focus on the main issues which are possible to assess based on the available data provided by Google and previous data identified in the literature review. They are going to be compared with the findings of EU MS competent authorities in Section 11.1, below.

10.10.2.1 Roles and responsibilities

940. When it comes to core services, Google makes a further rather artificial distinction between “information you provide or create with the core services (customer data)” and “information we collect when you use these services (service data)”. The distinction between customer data (data provided directly by schools, educators, students, or their parents) and service data (any other data collected by Google, such as observed data or inferred data) reinforces a narrative previously identified by Lindh and Nolin (2016). The data directly associated with the service’s benefits (front end) are presented and handled differently compared to the data more closely related to the back-end activities (and, therefore, to Google’s business model). The use of the term “service data” gives the impression that the collected data is not personal data and would not directly affect data subjects’ fundamental rights. This division adds an extra layer of complexity for schools, in addition to the existing one between core and additional services.

941. Google states that customer data provided or created within core services are processed according to the school’s instructions and does not mention the possibility of using them for its own purposes. In a separate section, Google mentions that service data are subject to the Google Cloud Privacy Notice. Unlike the case of customer data, there is no mention of Google acting under the school’s instructions (thus implying that schools are data controllers under LGPD). Given that the Google Cloud Privacy Notice is generic and applicable to all Google Cloud users (not necessarily just schools), there is also no mention of the respective roles and responsibilities regarding the protection of personal data between schools and Google.

942. Some of the aforementioned research sought to obtain, through information requests, the contracts made between states and municipalities and Google (Derechos Digitales; Privacy International, 2022; Núcleo de Informação e Coordenação do Ponto BR, 2022). Among the documents obtained, there were no agreements between the school and Google regarding the responsibilities of each party and how the data would be processed based on schools’ instructions. On the contrary, contracts were often signed directly online without any discussion about its clauses and necessary adaptations for the context of each school. This situation was also observed by the AEPD in one of the Spanish cases described above.

943. It is certainly possible that such documents exist but are not shared publicly, especially if they contain sensitive information. However, this scenario is highly unlikely, as this kind of document was not even mentioned in any of the responses, not even to state its unavailability.

Some public officials even claimed that the use of the platform did not entail personal data processing, which shows that data protection was not a concern. Thus, it is highly unlikely that Brazilian schools have real control over the purposes and means used to process personal data. At the very least, this would call into question the role of Google as a processor in the case of customer data and as a sole controller when it comes to service data.

944. Regarding additional services, the same division between data provided/created and data collected by Google is also applicable. However, in relation to these services, Google does not make any distinction regarding the responsibilities between the school and Google, which implies that it considers itself a controller for the processing activities within both types of services.

10.10.2.2 Purposes for processing personal data

945. The processing purposes described in the Google Workspace for Education Notice are provided in a non-exhaustive way. Data are processed to “provide, maintain, and improve services offered to students and schools; make recommendations to optimize the use of services; provide and improve other requested services; provide support; protect users, the public, and Google; and comply with legal obligations”.

946. They should be complemented by the purposes described in Google’s general Privacy Policy and Google Cloud Privacy notice when it comes to service data within the core services and all data within additional services. These purposes are also non-exhaustive and include processing data for providing, maintaining, and improving services; providing personalized services; measuring performance; communicating with the customer; and protecting Google, its users, and the public.

947. In the Google Workspace for Education Privacy Notice, Google underscores that core services are free from advertisement, and data is not processed for this purpose in other services. On the other hand, additional services may display advertisements, but are not personalized when these services are through accounts created by primary and secondary schools. Contextual factors like searches, time of day, or the content of the page content the student is viewing may still be used to tailor advertisements.

948. It is important to mention that, based on the principle of the best interests of the child and the guarantees provided in the CRFB, the CDC, and the ECA, advertising to children (whether based on their personal data or not) is prohibited in the Brazilian legal framework, and

such practice may also be considered abusive concerning adolescents (Henriques *et al.*, 2021; Henriques, Meira, *et al.*, 2020).

949. As will be emphasized in the section on transparency obligations, the purposes for which data are processed are extremely vague and non-exhaustive, which hampers the exercise of data subjects' rights and the analysis of compliance with various other parts of the LGPD.

10.10.2.3 Lawful Bases

950. In its ToS for Google Workspace for Education, Google states that schools can enable or disable any additional services at any time through the Administrator Console. Additionally, it states that they must “obtain parental consent for the collection and use of personal data in any Additional Products that the Customer intends to enable before allowing End Users under the age of 18 to access or use such Additional Products”.

951. This statement brings with it many complexities that must be carefully analyzed. First, if Google considers itself a sole controller for the data processed within additional services, it should be the one responsible for selecting the appropriate legal basis for processing the data. If consent were at all applicable, Google should be the one to collect it based on its direct relationship with the user.³³

952. Another issue that arises is related to the choice of consent for processing personal data within additional services. Considering the asymmetrical relationship between schools and students/their parents, and that education is mandatory in Brazil, it could not be considered freely given. Even if that were the case, it is difficult to identify how this would be operationalized in practice without violating other fundamental rights of children. Would the school have to provide different activities for students who do not consent to the use of additional services with their school account? How could this be implemented when the activity takes place in a group? What are the risks of the child facing discrimination at school?

953. Another issue is that, as discussed earlier, consent as a legal basis for the processing of personal data can be provided by individuals over 12 years old according to LGPD, not 18 years old. Thus, if this were an applicable and lawful basis in the specific case, Google could be

³³ As previously discussed in the EU cases, Google's access to data within additional services is facilitated by its legal relationship with schools. Consequently, schools would need to be considered joint controllers in this scenario.

violating the informational autonomy of adolescents by requiring parental consent, considering that it is their right to provide it independently.

954. Considering only the documents provided by Google, it was not possible to identify the legal basis used by schools to process student data through Google Workspace for Education in the core services as a controller or in the additional services if considered a joint controller. Most likely, according to the legal bases available in LGPD, schools would need to process them based on art. 7º, III (data processed by public administration, which are necessary for the execution of public policies provided for in laws and regulations or supported by contracts, agreements, or similar instruments).

955. The Google Cloud Privacy Notice does not provide a clear list of the legal bases used for processing personal data, which unfortunately is not legally required by LGPD. In some sections of the documents, it is possible to infer that data are collected, for example, to fulfill legal obligations (in a section focused on the purposes of data processing), or consent (in a section focused on occasions when personal data will be shared with third parties).

10.10.2.4 Transparency obligations

956. According to art. 9º, LGPD, data subjects must have easy access to information about the processing of their data, which must be made available in a clear, appropriate, and conspicuous manner. It also lists the minimal information that should be provided to the data subject, including (a) the specific purpose of the processing; (b) the form and duration of the processing, while respecting commercial and industrial secrets; (c) the identification of the data controller; (d) contact information of the data controller; (e) information about the use of shared data by the data controller and its purpose; (f) the responsibilities of the agents who will carry out the processing; and (g) the rights of the data subject, with explicit mention of the rights contained in art. 18, LGPD. Apart from art. 9º, the controller should also consider art. 14, §6º, as explained above, when children's data are being processed.

957. In this section, I provide a brief analysis of the privacy policies applicable to Google Workspace for Education in Brazil, focusing both on their content and format in relation to transparency obligations. It is worth noting that art. 9º, LGPD, stipulates the issuance of guidance by the ANPD for compliance with the principle of free access. This guidance would discuss how this provision should be implemented, but it has not yet been issued. Therefore, it is not possible to define in advance the level of detail that will be required by the authority

regarding each of the items listed in the provision. It is already possible, though, to observe some inconsistencies between Google's policies and the LGPD, which will be discussed below.

958. When it comes to the format, the documents schools must agree to in order to use Google Workspace for Education are structured through engaging titles, and the language used can be considered appropriate for an average adult, with minimal legal jargon. Throughout the documents, certain icons and images related to the subject matter are used, which facilitates understanding, although this is not consistently applied across all sections.

959. Certain words and expressions also contain hyperlinks that redirect the reader to specific articles, providing more detailed information on certain topics. This is an interesting technique to provide both conciseness and the necessary detail, depending on the level of information sought by the user.

960. However, as previously explained, understanding how students' data are processed requires consulting at least seven different documents, which is a significant number by today's standards. Moreover, one of them is not translated to Portuguese (the Cloud Data Processing Addendum (Customers)), which can severely hinder the understanding of information by Brazilian schools and data subjects, as most of the country's population does not speak English.

961. Finally, it should be highlighted that the documents are the same for adults and children. Although the language may be considered suitable for adults, the same cannot be said for children, who will have limited comprehension of the provided information. Considering the wide range of different children who have access to the platform in the country, with different ages and backgrounds, it cannot be said that the policy complies with art. 14, §6º, LGPD, by presenting information in a simple, clear, and accessible manner, considering the user's physical, motor, perceptual, sensorial, intellectual, and mental characteristics. Audio-visual resources are also not used in a way that provides the necessary information to parents or legal guardians and is suitable for the child's understanding, as the same article mandates.

962. Regarding the minimal content that should be provided in the privacy policies, it is generally scattered around the different documents. As stated above, the specific purposes for processing data are listed in the Google Workspace for Education Privacy Notice, Google's general Privacy Policy, and the Google Cloud Privacy Notice. The applicability of each of the policies depends on the type of service (if it is a core or additional service) and the type of information that is collected ("customers data" or "service data"), which can already be confusing for the schools and the data subjects. Even when compliance with a requirement was

verified in one of the policies, this was not always the case for the others. This continues to be a violation of the LGPD, considering that the documents apply to different services and data processing activities.

963. As specified above, the lists of data that are collected and the purposes of the processing are not exhaustive and worded in vague terms such as “provide, maintain and improve the service”, “develop products” etc. While the extent of information required by the ANPD remains unknown, it is evident that the current level of abstraction is maximal. Given the limited details available, data subjects face challenges in effectively exercising their rights and maintaining control over their data. Beyond sparse examples scattered throughout the policies, Google fails to specify the form and duration of data processing, a deficiency that already violates Article 9, b, of the LGPD

964. The same observation applies to roles and responsibilities within the context of data processing. Not only do the policies fail to clearly delineate the roles, but they also do not specify the responsibilities of each party, particularly in cases of joint-controllership, nor do they provide guidance on whom the data subject should contact to exercise their rights. In instances where the school assumes the role of controller, this must be explicitly stipulated in a privacy policy drafted by them. However, this does not seem to be the case with the educational secretariats consulted in the aforementioned research.

965. In instances where Google is considered the controller, its identification and contact information (items c and d) are not directly available. While the Google Cloud Privacy Notice does specify the name of the data controller in Brazil, accessing this information is not straightforward. To address any uncertainties regarding the policy or to exercise their rights, data subjects must navigate through the Privacy Center. Here, they encounter numerous questions and answers about Google’s privacy policies. After several clicks, they can eventually access a data access form, which seemingly does not cater to other rights under LGPD and is only available in English.

966. In the analyzed documents, Google does not include information about the data shared with it, which constitutes a violation of art. 9º, LGPD. Despite detailing the circumstances under which data is shared with third parties, it fails to include a list of these partners. While this information is not explicitly mandated by art. 9º, LGPD, it would be crucial for effective data control. Even when the data subject is aware of the content of Google’s privacy policies, it holds little value if the individual is unaware of whom their data are shared with, hindering their

understanding of how these partners process personal data. Thus, it can be argued that this lack of disclosure violates the principles of transparency, accountability, and good faith outlined in art. 6º of the LGPD.

967. Finally, the rights of the data subject as outlined in art. 18, LGPD, are also not detailed in the policies. Reference to the Brazilian framework is found only once in the Google Cloud Privacy Notice and is absent from both the Google Workspace for Education Policy Notice and Google's general Privacy Policy. The latter contains information on how to exercise the data subjects' rights if the GDPR applies to the processing of data, but it does not mention the requirements of the LGPD.

Interim Conclusion

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

969. This chapter aimed to describe the role of Google Workspace for Education in both the EU and Brazil and the impacts it brings to children's data protection in both jurisdictions. Considering the existence of decisions by EU competent authorities, there exists a natural filter that allows a more detailed analysis of these issues. In the Brazilian case, the lack of a specific decision on the matter demanded an analysis of publicly available documents provided by Google and previous research published on the subject.

970. Although both jurisdictions feature very similar data protection laws, they significantly differ in their levels of maturity regarding data protection culture. While the EU has had special laws since the 1970s, Brazil issued its first law in 2018, with enforcement beginning only in 2020. This implies that the ANPD and other competent regulatory bodies (such as consumer protection agencies) are still consolidating and adjusting to the new reality, significantly affecting the application of the law and its integration into people's daily lives. Nevertheless, the divergence in Google's approaches across these closely related jurisdictions speaks volumes about its intentions to expand its collection of personal data.

971. The next chapter will analyze the information outlined in this chapter, not only through a lens of compliance with the GDPR and LGPD, presenting convergences and divergences in the measures adopted in each country but also from a perspective of data colonialism, delving deeper to grasp the prevailing gaps in the current model that still allow data to be processed contrary to children's best interests.

Chapter 11. Analysis

972. After introducing Google Workspace for Education and its main features in Chapter 9, Chapter 10 was dedicated to delineating the challenges it poses to children's rights to privacy and data protection in the EU and Brazil. This was achieved by outlining the primary issues identified in Europe by competent authorities and, in the case of Brazil, by analyzing Google's ToS and privacy policies alongside previous research on the topic.

973. This chapter goes deeper by analyzing these cases data to find convergences, divergences, and gaps. I will first focus on the insights that can be gathered from the decisions of EU MS competent authorities, as well as from the description of how data is processed within the Brazilian reality. This analysis will be structured around the main aspects of data protection laws that are in tension with the identified challenges. The second part of the chapter aims to understand these cases through the lens of data colonialism. Challenges mapped in Chapter 8 will also be useful to situate the discussion and derive conclusions that hold relevance for other edtech.

11.1 Tensions between the GDPR, LGPD and Google Workspace for Education

974. The decisions of EU MS competent authorities outlined in the previous chapter, along with the operation of Google Workspace for Education in Brazil, shed light on systematic concerns regarding children's data protection in the adoption of this technology by public schools. This section is dedicated to pinpointing the primary areas within the GDPR and LGPD that may conflict with the implementation of Google Workspace for Education, while also delineating possible convergences, divergences, and gaps.

11.1.1 Roles and responsibilities

975. A very important topic that stands out in almost all EU decisions and the Brazilian case is the difficulty in delimiting the roles and responsibilities of schools and Google regarding the processing of personal data. This discussion was very clear within the Dutch case and the contracts analyzed by Privacy Company. Google qualified itself

as [a] data processor for the personal data in Customer Data it processes through the Core Services in G Suite (Enterprise) for Education (described as the Customer Data in this DPIA) [and] as data controller for the Google Account, most of the Additional

Services including Chrome OS and the Chrome Browser, the Diagnostic Data and other services related services such as Feedback (Nas, Sjoera; Terra, 2021, p. 6).

976. For other services, the roles were considered not to be clearly defined or were unlawfully designated. Google could not be considered neither a sole controller nor a processor for some activities. It had access to some personal data only because of its relationship with educational institutions, meaning that there should be a joint controllership relationship according to the EDPB guidelines. The joint controllership was, however, not a possibility in cases when the purposes of the data processing were not aligned with the legal duties of the school to provide education, something also identified by the Danish DPA. The only situations where this would not apply would be when Google processes data for its own legitimate business purposes, like invoicing, or when they are required to disclose data to authorities (in cases where Google is not able to forward this request to schools) (Nas, Sjoera; Terra, 2021, p. 107).

977. A situation mirroring that identified by Privacy Company could be seen in Brazil. Upon reviewing the ToS and privacy policies applicable to the country, the only certainty we have is that Google considers schools as controllers when it comes to customers data (information directly provided by schools or data subjects when using their services) within core services. Their roles and responsibilities concerning service data in core services and all data in additional services remain unclear, although it can be inferred that Google considers itself as a controller in these contexts.

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

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

980. In the Finnish case, the DPA found that by accepting Google's ToS as it was, the controller undermined its ability to adequately control and supervise the processing of personal data, a concern also recognized in a previous DPIA. Similarly, in the Danish case, the Helsingør

municipality was unaware of many changes made by Google to its ToS, which contributed to a breach of students' data. Lastly, the VTC in the Belgian case also highlighted that the purposes and means of processing personal data could change at any time when Google modifies its ToS, posing a concern for schools.

981. The common thread connecting all the issues above is the factual influence exerted by Google on the purposes and means of the processing activities. As controllers, schools bear the responsibility to ensure that the processor adheres to data protection laws and implements necessary safeguards. Regarding AI systems, schools must understand how they work and make decisions, as they must explain this information to data subjects (ICO, 2022).

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

983. Even if schools agree with the purpose of the processing, it must be verified whether Google is actually deciding essential means such as which data is processed; for how long they are processed; if decisions are automated, etc. Given the often limited expertise of schools in understanding the operations of AI systems, especially when trade secrets are involved, and the lack of explicit prior instructions provided to Google (depending on how the ToS have been signed and the influence exerted by the schools on its terms), a scenario where Google is considered a joint controller in these cases becomes a possibility. The discussion in such cases would also demand consideration of appropriate legal bases.

11.1.2 Purposes for processing personal data

984. Defining the purposes for which personal data are processed is a crucial step towards compliance with the GDPR. Transparency regarding these purposes is essential to ascertain adherence to principles such as purpose limitation, data minimization, lawful processing, among others. The cases narrated above show that the purposes for which student data were processed were not clear, especially when Google was the controller for the processing activity.

985. The Brazilian case stands out as particularly relevant in this context, given that the ANPD has not yet provided guidance on the level of detail required in the information to be provided to data subjects. Nevertheless, it is evident that the information currently available

regarding the purposes of processing personal data is excessively vague and incomplete. This lack of clarity makes it difficult, if not impossible, for data subjects to effectively exercise their rights, which shows that the available information is not fulfilling its intended functions.

986. In two other cases, Germany and the Netherlands, the irregular processing of telemetry and diagnostic data was specifically highlighted. Telemetry data refers to information obtained through telemetry, a process involving the automatic collection, transmission, and measurement of data from remote sources using sensors and other devices. Even though some level of pseudonymization is applied, telemetry data can still contain elements that could be used to identify individuals, which can be considered personal data. Diagnostic data are often collected through telemetry, providing insights into the devices employed and the performance of the applications used (Hessel, 2022).

987. At the time of the first DPIA carried out by Privacy Company, Google had not made available any public documentation regarding the specific purposes for which it processes diagnostic data, whether to be used in core or additional services. Just as in the case of the collected data, information about all the purposes for which Google processed data was also not clearly and thoroughly available, especially when Google was acting as a data processor (Nas, Sjoera; Terra, 2021, p. 6). Although the narrative behind the use of diagnostic data is often linked to the implementation of security measures on the platform, the lack of clear purposes means that one cannot be sure of their beneficial use.

988. The separation of core services and additional services, as well as customer data and service data, may initially be perceived as positive, as it allows Google to distinctly delineate controllership, thereby specifying the entities responsible for determining the intended purposes. However, the Dutch case, where multiple DPIAs have been carried out, has shown that this separation is not straightforward and can be difficult to operationalize in practice. Even when schools were required to disable additional services (as they are not in control of the processing of data and Google would not have a legal basis to process them in that context), students would often create personal accounts to use them, ensuring a smoother integration between services.

989. The DPIAs also highlighted that the data flow between accounts and among core and additional services lacked clarity. Consequently, even when the school initially defines the purposes for processing student data, the structure of the services facilitates the collection of data for commercial purposes.

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

991. Finally, there was little or no discussion in relation to the use of AI systems within Google Workspace for Education and how the purposes of processing personal data were impacted. If data were collected to provide the service to schools and is being further used to train AI or improve Google's service, a careful analysis of art. 6(4), GDPR, would be imperative.

11.1.3 Lawful Bases

992. The appropriate legal basis for processing data related to Google Workspace for Education by schools was widely discussed by the EU MS authorities. Some cases were brought to their attention due to complaints regarding the absence of parental consent for schools to process data within the platform. The Danish DPA clarified that the Municipality's use of art. 6(1)(e) of the GDPR was correct, and consent was not applicable] for the provision of Google Workspace for Education Core Services and the creation of individual user accounts within the platform.

993. In the Norwegian case, some municipalities relied on consent, the performance of a contract, and the legal obligation to process students' data. However, the DPA determined that in all cases, the appropriate legal basis should be the task carried out in the public interest, as outlined in art. 6(1)(e) of the GDPR. Similarly, in the Finnish case, the authority concluded that relying on a legal obligation was not lawful, as the Finnish Education Act lacked specificity and did not mandate the use of digital technologies. Consent was also deemed inappropriate since data subjects would not be able to provide it freely.

994. Although not much detail has been provided within the publicly available decision, the case discussed under the Hessian DPA's jurisdiction briefly mentioned the fact that consent should not be used as a legal basis to justify the use of cloud services such as Microsoft Office 365 and Google Workspace for Education.

995. In Spain, the authority provided two different opinions on the matter. In one instance, the AEPD determined that consent was not suitable as a legal basis for processing students'

data under Google Workspace for Education by schools, as requested by the complainant, due to the power imbalance between the school and the data subjects. In this case, the appropriate basis would also be art. 6(1)(e), GDPR. Nonetheless, in a very similar case, the authority did not consider consent as an inappropriate legal basis but still deemed it invalid due to the lack of adequate information provided to the data subject.

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

997. Within the EU, most of the cases indicate that art. 6(1)(e) is the most appropriate legal basis to be used when schools are processing data as controllers within the deployment of Google Workspace for Education. In cases where Google would like to process personal data for their own purposes, such as within additional services, a new legal relationship between them and the data subjects must be established, and a new legal basis defined. An important issue remains, however, regarding the data that Google has access to only because of its relationship with schools. If data is used for training AI, for example, the question remains whether schools could be recognized as joint controllers as this would probably not fall within their responsibilities as public entities and, therefore, the legal basis of art. 6(1)(e).

998. A similar issue was also observed in Brazil. Since the reviewed documents only comprised those publicly disclosed by Google, it remained unclear which legal bases schools relied upon to process children's data within the platform when acting as controllers. Google's privacy notices did not provide a clear enumeration of legal bases for their processing activities. However, within its ToS for Google Workspace for Education, Google stipulates that schools must "obtain parental consent for the collection and use of personal data in any Additional Products that the Customer intends to enable before allowing End Users under the age of 18 to access or use such Additional Products." As previously discussed, this statement raises significant concerns. Not only does Google assume the role of controller in this scenario, but relying on consent may fail to meet crucial criteria outlined in the LGPD, such as being freely given and ensuring compliance with age of consent requirements.

11.1.4 Transparency obligations

999. The provision of information to data subjects under arts. 12-14, GDPR, was also subject to analysis in some EU cases. In Norway, the Municipality in question held a meeting with parents, where information regarding the processing of data was said to be presented. The DPA was of the opinion that having this type of meeting or only referring to Google's ToS was not sufficient and should be supplemented by information in writing, especially considering the services being targeted at children. This is particularly important when Chromebooks can be used for private purposes with private accounts.

1000. In Spain, the AEPD considered that the documents provided to parents were insufficient to comply with the information requirements in the GDPR. Key information was missing from the documents, and they were not written in a language that children, as data subjects, could understand. In the case of Finland, the DPA found Google's ToS general and difficult to interpret, meaning that there was a risk that the processing activities were not properly defined.

1001. It is important to emphasize that Google's ToS establish a relationship and are binding between the school and Google. In cases where the school is a controller, it must provide appropriate information to the data subjects and include how it also processes student data beyond what was agreed upon with the processor. This information must be aligned with the understanding of children when they are the data subjects.

1002. In the Brazilian case, it was not possible to ascertain the information that schools were providing to data subjects. However, the review of ToS and privacy policies applicable to Google Workspace for Education in the country revealed a lack of essential information as mandated by the LGPD.

1003. First, pertinent information regarding data processing is scattered across different documents, some of which are solely available in English. The documents are the same for children and adults alike, which directly infringes art. 14, §6º, LGPD. Concerning their content, details about the data collected and the purposes for their collection are vague and incomplete. Data subjects are not afforded the option to access additional information if desired, and crucial details such as the duration of data processing, the respective roles and responsibilities of Google and schools, data sharing practices, and procedures for exercising data subject rights are notably absent.

1004. In a similar exercise of reviewing Google's ToS and privacy policies, Hooper *et al.* (2022) emphasized the large number of documents and legal terms (over 60) that schools must

navigate in order to understand Google Workspace for Education's activities. Determining which one is applicable mainly depends on the context and services used by the school. The same conclusion was reached by Marrafon and Fernandes (2020) while analyzing the 2019's policies applicable to the Brazilian reality. The policies were scattered, many of them only available in English, and the actual implementation of each one was challenging to define. This gets even more difficult when third-party apps are used within Google Classroom through its API, as mentioned above.

11.1.5 DPIA and risk assessment

1005. The EU cases described above show how important and yet challenging it can be for educational institutions to assess the risks to the rights of the data subjects involved in the data processing. Most cases discuss the need to carry out a risk assessment on the security of data processing (art. 32, GDPR), and/or a DPIA (art. 35, GDPR).

1006. In relation to the obligations under art. 32, GDPR, the Danish DPA found that the Helsingør Municipality should have conducted a risk analysis to identify the risks that access to Google Workspace for Education's additional services would entail. In that case, it meant that students' personal data were being displayed when they used YouTube. In the Norwegian case, the DPA found that when acquiring hardware and software to be used in education, municipalities have an obligation to carry out a risk assessment based on art. 32, GDPR. Although some of the municipalities have done so, it was not considered sufficient as they have not implemented safeguards to keep themselves up to date about the changes in Google's ToS.

1007. Although the actual list of processing activities that are considered high risk differs from authority to authority, there is a high degree of convergence in the cases presented above. The Danish DPA found that the Municipality in question should have carried out a DPIA because it involved new and complex technology and data from children were being processed. The authority considered that the risk was especially higher because the technology was implemented within the scope of education and because other products offered by Google were financed by targeted advertisement and selling of information. The first two reasons were also mentioned by the Norwegian DPA due to the application of a new technological or organizational solution (in that case, the use of cloud services in primary schools) and the processing of personal data of vulnerable data subjects.

1008. The lack of a DPIA constituted the main reason to initiate investigations within the scope of the Swedish DPA. Although the controller had conducted a DPIA when the service was first implemented in 2014, it failed to review it in 2020, when the service was migrated to the controller's own IT environment. The IMY considered that the case would fulfil two criteria for carrying out a DPIA, namely the large-scale processing of data and the processing of data pertaining to vulnerable individuals.

1009. The first case brought before the Spanish DPA highlighted the incompleteness and inadequacy of the conducted DPIA. Although the assessment had been carried out using a template furnished by the authority, it failed to account for the unique aspects of the case, notably the processing of children's data.

1010. Finally, the Dutch case stands out when it comes to performing a DPIA. Of all the cases, this was the most comprehensive one and delved the deepest into the specifics of the technology. This was only possible due to the DPIAs and audits conducted by the Privacy Company on behalf of educational institutions. Several risks were only identified through these analyses, which most likely would have also emerged if they had been conducted in the cases discussed by other DPAs. This illustrates that conducting well-executed DPIAs is extremely time-consuming and financially demanding, which may not necessarily be feasible for schools in other situations. Furthermore, it demonstrates that despite modifications made by Google, these changes led to the need for new assessments, uncovering additional issues.

1011. Thus, more than just a step in the adoption of technologies, the DPIA should be something carried out constantly, especially when there are changes in the technological or organizational situation. In a situation where the company offers standard ToS for schools and has the prerogative to change them at any time, the latter find themselves in an extremely complicated situation. This prompted the Belgian authority VTC to assert that for schools, conducting DPIAs is not merely difficult but frequently unfeasible. Apart from the shortage of human and financial resources necessary for such undertakings, schools also lack real visibility of the risks posed by the technology. The collaborative decision-making model identified in the Netherlands and Denmark, for example, where human and financial resources are pooled, may be an effective way to address this problem. Furthermore, focusing on technologies over which the state and schools have more control can also help solve it.

11.1.6 Data Transfers

1012. Data transfers between the EU and third countries can be carried out under certain circumstances defined by Chapter V, GDPR. In the case of the US, this has been historically legitimized by adequacy decisions based on art. 45, GDPR. However, the situation has become increasingly complex over the years, due to invalidations of these arrangements by the CJEU. Two main challenges in this regard were identified by the Court, namely

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

1013. In the analyzed decisions within the EU, the transfer of data to the USA emerged as a recurrent theme. In the Dutch case, the Privacy Company's 2021 DPIA found that the only two relevant differences between the free and premium versions of Google Workspace for Education were additional security measures and the option to select EU data center storage for specific Core Services. Nevertheless, certain data processing activities, like providing technical support to users, might still involve transfers to the USA.

1014. As a result of the jurisprudence in Schrems-II and of the EDPB measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (EDPB, 2021), schools would need to perform a risk analysis of the transfers outside the EEA. In the Netherlands case, it was unclear if schools would be able to use Standard Contractual Clauses (SCC) due to the change of the definition of international transfer in the SCC published by the Commission in 2021. If that were the case, schools would be required to implement supplementary measures to guarantee compliance with the EU's standards for safeguarding personal data. The same was identified in the Danish and Finish cases.

1015. The EDPB recommends the employment of strong encryption as the best measure to mitigate the risks associated to unlawful processing when transferring data outside of the EEA. Although the municipality in the Danish case argued to use encryption when data was transmitted and processed by Google, it was not considered strong enough by the DPA, as Google could still access the information in plain text.

11.2 Appropriation of resources through the lack of compliance with the data protection framework

1016. An important element of data colonialism, as described in Chapter 3, is the appropriation of resources. Data are seen as readily available and abundant, much like a natural resource such as oil or minerals. This perspective leads to the perception that data can be harvested, exploited, and used without considering the implications or consequences for the individuals and groups from whom the data is collected. Just as historical colonial powers exploited land, natural resources, and labor from colonized territories, the social quantification sector may similarly exploit data without sufficient regard for people's rights to privacy, data protection, and autonomy.

1017. Viewed through the lens of data commodification, data are perceived as traces left behind by individuals or groups when utilizing technology, as something that naturally exists, representing missed opportunities if not adequately harnessed. However, as we have previously discussed, data always result from an abstraction process, one facilitated by specific design choices.

1018. As discussed in section 11.1, non-compliance with data protection regulations is an important means to guarantee that more data are available for the company's commercial purposes. Both Google and the public entities using its services have failed to adhere to fundamental rules outlined in the GDPR and LGPD. This was particularly evident in the Netherlands and Denmark cases, where more comprehensive investigations into the technology's functionality were conducted, either through third-party DPIAs or by the DPAs themselves.

1019. The lack of compliance is generally disguised by very specific narratives that help justify data colonialism, which is also one of its main aspects as highlighted by Couldry and Mejias (2019). Apart from this broader narrative of data commodification, the strategy adopted by Google is related to what Lindh and Nolin (2016) define as a front end/back end strategy. While the service's advantages are evident to users (front end) such as free services and interoperability, the back-end activities are relatively hidden by a specific narrative. The authors have analyzed Google Apps for Education's (now Google Workspace for Education) policy documents and concluded that they had the aim of "disguis[ing] the business model and persuad[ing] the reader to understand Google as a free public service, divorced from marketplace contexts and concerns" (Lindh; Nolin, 2016, p. 650). This is done through many

different tactics such as focusing on the benefits for user experience (benefiting rhetoric) and framing practices related to their business model as minor aspects of their activities (side-lining rhetoric) (Lindh; Nolin, 2016). As observed, it also involved using specific language that fosters the perception among users that the information Google collects is not personal data, but “service” data.

11.3 Unequal data relations and global distribution of the benefits of resource appropriation

1020. Apart from the appropriation of resources, justified by specific narratives, data colonialism is also embedded in unequal social-economic relations and unequal global distribution of the benefits of resource appropriation. Although these are two separate components, they can certainly be identified together in the cases described above. Chapter 9 has described Google Workspace for Education and the business model it relies upon. It showed that the data relations established by Google and schools are unequal for several reasons.

1021. First, it is important to emphasize that providing digital technology solutions for education is not Googles’ main activity. Google’s business model is primarily based on data harvesting and targeted advertising. Some view Google’s offer of this edtech for free as a genuine act of charity, something the company does to fulfill its social role in the world and improve it. While this may indeed be part of a broader justification for its provision (see discussion in Chapter 9), the facts above demonstrate that children’s data have been processed for purposes contrary to their best interests. The true intention behind the technology, or the narrative presented by the company, loses significance when such evidence is brought to light.

1022. As stated in the mapping exercise conducted in Chapter 8, the very way AI systems operate brings several challenges to the exchange of necessary information between data controllers and processors. It is not easy to identify which data have been used by these systems to draw inferences or make decisions, as well as the weight each piece of data has. Schools generally lack the expertise and resources required to obtain relevant information about their operation, not only to procure the service but also to ensure its compliance with data protection rules and the best interest of children. The opacity of the operations conducted with personal data, therefore, not only interferes in several rights put forth in the data protection frameworks, but also increases the power imbalance between schools and edtech providers.

1023. This is even more serious in the Brazilian context, where the lack of investment in education and sovereign digital infrastructure makes partnering with companies that provide

their products “for free” much more attractive. During the pandemic, when states and municipalities had to switch from in-person to online classes overnight, employing these technologies was the only way to maintain educational activities. Therefore, data colonialism feeds into a vicious cycle. By adopting free education technologies, the investment in sovereign technologies is further neglected and the possible available budget passed on to other sectors.

1024. It further emphasizes the influence wielded by the social quantification sector over individuals as a whole. This is evident as the accumulation of data enables deeper insights to be extracted, thereby amplifying the potential for manipulation by these entities. This is even more problematic when it comes to educational data, which are so valuable within a human profile and so indicative of a country’s human capacity and resources.

1025. The power imbalance among the involved actors also results in the benefits of data appropriation being concentrated in the hands of the social quantification sector. Considering the provision of technology by private actors, any crucial insight that can be derived from data collected within education remains restricted to the information that the company is willing to share with the government. Public entities lose the capacity for adequate analysis of the implemented public policy and the use of data for other purposes aligned with children’s development and education.

11.4 Digital sovereignty

1026. We have discussed above the key elements of data colonialism, how it manifests, and how it could be identified through the mapping of challenges undertaken in the preceding chapters. It is now essential to delve deeper into something that underlines these aspects, which has been directly addressed in certain EU cases and is closely linked to some of the potential solutions that will be highlighted in the conclusion of this thesis.

1027. The cases mentioned above all involve elements of digital sovereignty, a critical concept associated with the imperative to bolster the autonomy of individuals and society in the face of data colonialism. The German case in Hesse, for instance, gained attention due to Microsoft’s announcement that its services would no longer be delivered through a German cloud. This implied that the state’s control over the data processed by these services would be affected, prompting a reconsideration of other services, such as Google Workspace for Education. In a similar fashion, France decided that Microsoft and other cloud services like Google do not comply with its Cloud at the Center doctrine, and their provision of free services would also

impact competition and be contrary to public procurement rules. The Danish, Dutch, and Finish cases relied on digital sovereignty arguments while focusing on Google Workspace for Education's compliance with data transfer requirements outlined in the GDPR, particularly in light of the latest developments on this matter within the CJEU.

1028. Discussing digital sovereignty solely through the lens of competition, data localization and data transfers can be narrow, and other aspects should be highlighted. After providing a brief definition and main aspects of the concept, I will analyze additional elements that could have been identified by the authorities, which can be highly significant for the development of digital sovereignty also in the Brazilian context.

11.4.1 The concept of digital sovereignty

1029. The modern concept of national sovereignty is based on an analog world, and encompasses the power exercised by the state on all affairs within its territory, such as its resources and people. The digital environment, however, puts tension on this concept, as it lacks physical boundaries and is mostly subjected to private forces, especially multinational corporations, which makes it increasingly globalized (Floridi, 2020, p. 372). Therefore, rather than being just a subcategory of sovereignty, digital sovereignty affects the core of political institutions and their very ability to exercise sovereignty in a broader sense (Smuha, 2023a, p. 3).

1030. Digital sovereignty can be understood as the “control of the digital”, i.e., the ability not only “to influence [it] (e.g. its occurrence, creation, or destruction), [but also] its dynamics (e.g. its behavior, development, operations, interactions), including the ability to check and correct for any deviation from such influence” (Floridi, 2020, p. 371). This could be understood in relation to individuals and their ability to shape the digital sphere in a self-determined way or in relation to states (Herlo; Ullrich; Vladova, 2023; Núcleo de Tecnologia do MTST, 2023).

1031. In the case of states, this can occur in two ways. First, by controlling the digital infrastructure, which includes capital resources (such as software, hardware, standards, and cables); intellectual resources (such as human resources and institutions); and financial resources to experiment and design new models and possibilities (Pinto, 2018, p. 17). Second, by controlling a country's destiny through public policies (Lefèvre, 2023) and norm-setting capacity (Smuha, 2023a, p. 8).

1032. The control of digital infrastructure is challenging, and will depend on the policies, political power, international pressure and influences, as well as resources available to each country. It requires understanding that allocation of resources to this area is essential for the existence of democracy and people power. This is enough to demonstrate how dangerous and detrimental short-term policies like accepting free services from foreign technology companies with data-driven business models can be. However, considering the broader context also involves recognizing that some countries have limited choices.

1033. Policies focused on the adoption of open-source software, for example, can be an interesting path in the case of countries with few resources (European Commission, Directorate-General for Education, Youth, Sport and Culture, 2021, p. 142), as, in addition to being free, it is open to public scrutiny. However, this alone is insufficient to build a robust digital policy in a given country. This inadequacy arises not only from the need to prioritize sustainability and achieve widespread adoption, but also from the pervasive influence of private entities and foreign states in shaping public policies through lobbying and manipulation. This demonstrates how the two types of control in digital sovereignty—economic and normative—are interconnected (Pinto, 2018, p. 21; Smuha, 2023a).

1034. The relationship between companies and states is also asymmetric in the digital age, with the latter frequently depending on the infrastructure provided by the former. Companies are currently the ones determining the nature and speed of technological change, while states' role is often perceived as being able to control its direction (Floridi, 2020, p. 371). However, this has not been the case for most countries, which already struggle to set this direction, let alone innovate and proactively consider what kind of technology serves best the public good and aligns with the state's strategies, such as through procurement mechanisms (Mazzucato, 2019, 2020).

1035. Controlling a country's or even a supranational entity like the EU's digital destiny through legislation and public policies can also be extremely challenging in a globalized world. This includes dealing, for example, with the intense lobbying of tech companies and foreign states in the definition and drafting of policies, investment plans, as well as in proposing specific legislation related to the digital domain. Defining digital strategies through policy can, for instance, be influenced by consultancy firms, which are increasingly moving from the sidelines to the center of important decisions within the public sphere. Their business models, underlying conflicts of interest, and lack of transparency are ever more a problem to our democracies and economies (Corporate Europe Observatory, 2023; Mazzucato; Collington, 2023).

1036. The AI Act serves as an important example of the influence on the legislative activities themselves. A report published by Corporate Europe Observatory, for example, showed how the EU's pioneering attempt to regulate AI has faced intense lobbying from USA tech companies. This happened not only through pressure from the corporations themselves but also through covert groups, tech-funded experts, and the USA Government (Schyns, 2023). These activities have been ongoing since the initial drafting of the act, and previous research indicates that this is not an isolated case (Bank *et al.*, 2021).

1037. Even when legislators are able to pass regulations, the latter still have their limits because of possible poor choices while legislating or the difficulties related to their enforcement (Massé, 2022; Smuha, 2023a). Therefore, more than regulating technologies themselves, it is important to actually regulate the incentives to undermine regulation, such as the widespread DDBM depicted above.

1038. Strengthening digital sovereignty is certainly not linked to anachronic notions of digital sovereignism or digital statism. It does not involve replacing a nation's sovereignty, it rather, seeks to complement it with a contemporary digital counterpart. This kind of digital sovereignty serves as a crucial enabling factor to sovereignty in general, offering a broader array of advantages, such as harmonization (including standards and requirements), ensuring a fair competitive environment, and fostering greater opportunities for coordination among all stakeholders (Floridi, 2020, p. 375).

11.4.2 Data colonialism actors and digital sovereignty

1039. Before considering how we can broaden the notion of digital sovereignty as identified in the cases above, it is first important to remember that the network of actors and powers involved in historical colonialism are not the same as in data colonialism.

1040. Despite being the protagonist of historical colonialism, Europe is also grappling with the adverse effects of data colonialism. The GDPR and, more recently, the European Data Strategy stand as clear illustrations of the EU's attempt to guarantee digital sovereignty and pursue a "third way", different from the laissez-faire USA approach and China's state-controlled model.

1041. Indeed, historical, social, economic, and cultural disparities—often remnants of historical colonialism—have resulted in more extensive identification and discussion of data colonialism issues in Europe. This includes not only data protection issues but also how big

tech companies' operations impact competition and the democratic discourse through disinformation and manipulation. The EU is trying to reverse its position in the world regarding digital technologies, investing in new legislation that seeks to give individuals and companies more control over their data, and directly in infrastructure based on European values, in order to reduce its dependence on foreign technologies.

1042. Heidebrecht (2022) is of the view that stakeholders and public authorities (rather than business actors), have gained greater significance in the EU's digital governance processes, leading to the introduction of more market-correcting instruments. In Section 6.3, I briefly discussed how, despite the importance of the EU data strategy for bolstering digital sovereignty, it may still be imbued with a narrative of data flow that is detrimental to individuals and society. It fails to adequately address the root causes of data colonialism, such as data commodification. Delving deeper into this topic unfortunately falls outside the scope of this thesis.

1043. On the other hand, most countries in the world are still trying to keep up with drafting and implementing basic legislation, such as personal data protection laws. Countries within the Global South have fewer material resources and political power available to independently shape their digital destiny and tame the social quantification sector, which is one of the reminiscences of historical colonialism. This includes the enactment and enforcement of new, stricter legislation, as well as the creation of a sovereign infrastructure that enables the implementation of new perspectives regarding the role of data in society.

1044. This is especially challenging within the current political scenario, where many of the pieces of legislation are "imported" from Europe, the GDPR being a great example of the Brussels effect. Although driven by good intent, this kind of universalism can ignore the particularities of each country, especially when it comes to their institutional design, social-economic situation and cultural specificities. Merely transposing legislation can be meaningless if strong enforcement mechanisms are not in place (Arora, 2019).

1045. On the contrary, the existence of stricter legislation without adequate enforcement can even legitimize harmful practices and hinder the demands for the realization of the most basic human rights. Within the context of Brazil, the

"[p]olitical, economic and social challenges have prevented, and still prevent, the construction of a complete citizenship [...]. Although influenced by the philosophical discourse of modernity, the adoption of legal models in Brazil has occurred, in various situations, in a particular and partial way, as in a real game of imitation, an incomplete and untimely simulacrum of never-realised expectations" (Negri, 2021, p. 8).

1046. This is especially interesting considering that, as I have shown in Chapters 7 and 8, the legal framework that governs personal data processing in the EU and in Brazil are extremely similar. The LGPD is based on the same structure, spirit, and principles of the GDPR, with only some specific differences. However, considering the existence of vulnerability layers and the material differences between the two jurisdictions, the laws are not necessarily applied equally.

1047. It must also be considered that these differences, although to a lesser extent, also exist within the EU. As will be discussed below, the decisions made in the region regarding Google Workspace for Education have mainly come from wealthier and more politically powerful countries that allocate more resources to education and personal data protection, therefore affording to be stricter with the social quantification sector.

11.4.3 A broader notion of digital sovereignty

1048. To expand the scope of digital sovereignty beyond the parameters delineated by EU competent authorities, we can identify interesting elements emerging from the decisions that go beyond competition and data localization/data transfer concerns.

1049. The first one is the very existence of resources that allowed for enforcement and negotiations with Google that led to amended contracts. In the case of the Netherlands, for example, the Government has been able to engage Google in months of highly technical discussions based on several DPIAs and deep analysis of the technology. This indicates that they have both capital and intellectual resources at hand to comprehend the implications related to the processing of children's data. The symbolic power of the Dutch DPA also played a significant role, as some even consider that certain USA tech firms now view the Dutch endorsement as a prestigious status symbol, as a seal of approval that they have navigated one of Europe's most rigorous data protection compliance procedure (Singer, 2023).

1050. Secondly, a centralized approach was key to enhance their bargaining power and making the solution scalable. They have demonstrated that this is possible not only by centralizing procurement activities within a specific government entity but through cooperatives of schools and universities. Most schools would not have the means, power, and expertise to independently audit technologies, so cooperatives represent their collective interest and preserve, at the same time, some of their autonomy. The same centrality through cooperatives was identified in the Danish case. One of the cases that took place in Germany, on the other hand, demonstrates the imbalance of power and the need for collective approaches. A

student in Dortmund refused to use Google Workspace for Education due to privacy concerns but faced technical and discriminatory issues within the school.

1051. However, it is essential to consider that focusing solely on the strategies outlined above, while crucial and indicative of the potential for effective enforcement of the GDPR, may not be sufficient to ensure the delivery of education in the best interests of children and in a manner that guarantees digital sovereignty.

1052. These negotiations do not address the core issue of data commodification/data flow paradigm and the market incentives related to the business model of big tech platforms. Children get used to these platforms and are continuously subjected to surveillance and detrimental practices as soon as they leave the controlled school digital environment. The persistence of the business model and incentives for massive data collection also mean that new risks can continuously arise, as highlighted in the most recent DPIA conducted in the Netherlands.

1053. The case of France, in this sense, is particularly noteworthy not only because it bans certain technologies based on a digital sovereignty perspective, but also because the decision was taken by the French Minister of Education and Youth. The possibility of making decisions including broader political considerations beyond the data protection framework (which becomes more difficult when this is done by DPAs), suggests that other elements beyond compliance should be considered.

1054. Lastly, entrusting crucial digital infrastructures to private entities often involves surrendering education-related data that could be used by governments and civil society in the best interest of children, such as to develop privacy-preserving technologies, as well as innovative and collaborate solutions to improve learning (Hooper; Livingstone; Pothong, 2022, p. 56).

1055. This is where digital sovereignty intersects with the imperative to challenge data universalism. We have observed how issues stemming from datafication, particularly certain business models, are systemic and global in nature. However, endeavors to identify solutions must consistently account for local specificities, encompassing both the material and cultural dimensions of knowledge production. It is essential to harness the full potential of each society to foster new imaginaries and conceive alternatives for the data future we aspire to build.

Interim Conclusion

1056. Chapter 11 aimed at analyzing the information described in Chapter 10 to uncover convergences, divergences, and gaps. I have focused on examining the primary areas of conflict with data protection laws, as well as how they can be understood through a data colonialism lens. This analysis exposes a consistent failure of schools and Google Workspace for Education to adhere to data protection frameworks in the EU and in Brazil, revealing challenges that transcend regulatory compliance.

1057. It also underscores the inherent challenges posed by the adopted business model, despite efforts made during negotiations to ensure compliance. Even if children's data are not processed for target advertising, they may still be leveraged for other commercial purposes not necessarily aligned with their best interests. Additionally, children are familiarized and nudged to continue using these technologies outside the school environment and throughout their lives.

1058. I have also discussed how a comprehensive understanding of digital sovereignty extends beyond issues of competition and data localization/transfer. The decisions taken within EU illustrate how the economic and political capital of the analyzed countries significantly influence their level of digital sovereignty, and, consequently, the decisions they can actually make. The social and economic disparities within the EU itself become evident as the countries in question belong to the wealthiest and most politically influential group in the region.

1059. While adequate enforcement remains crucial, both within the EU and Brazil, it alone may not suffice to deliver education in the best interests of children or to ensure digital sovereignty, at both individual and collective levels. A discussion on the appropriate purposes for which children's data are processed is needed. Entrusting essential digital infrastructures to private entities raises significant concerns regarding their business models and governance along with their potential short- and long-term impacts on society. There is a pressing need to challenge data universalism and collaboratively devise solutions that account for local specificities, while leveraging the unique potential of each community to explore alternative approaches in shaping the society we aspire to be part of.

CONCLUDING REMARKS

1060. This thesis aimed to investigate the challenges that edtech presents to children's rights to privacy and to the protection of personal data, and the extent to which the existing legal framework in both Brazil and Europe address them. In this conclusion, I will summarize the path taken to answer this question, along with the main findings and contributions of the research, which will be emphasized in italics for clarity and ease of reference.

1061. From a descriptive approach, **Part I** aimed to set the scene and discuss the context of edtech deployment. **Chapter 1** introduced and explained the concept of edtech, providing a historical perspective on the evolution of technology in education. The purpose of this historical overview extends beyond simply illustrating the steps taken for the current technologies to be available, viewing computers or AI technologies as the pinnacle of edtech technological development. Its primary aim was to discuss the methodologies and epistemologies behind previously adopted technologies that continue to shape contemporary technological paradigms. An important example in this regard was the development of so-called teaching machines, heavily influenced by behaviorist and mechanical views of education, which still impact how education is currently understood and delivered, especially concerning personalized learning technologies.

1062. I have also discussed the concept of education, which directly informed the analysis made in the previous chapters. More specifically, I have embraced a comprehensive understanding of education, essential for framing history and future as a possibility. By conceiving education as not only capable of shaping children's knowledge and skills but also influencing their worldview and ethical-political expressions, we recognize its profound impact on human intervention in reality and the development of their agency for effective change. *Recognizing education's transformative and multiplier role sheds light on the enormous power that edtech has on shaping society. This stresses the need to understand education and a highly political and strategic sector, which demands transparent, democratic, and fair decisions.*

1063. Given the vast quantity of technologies available, their diverse purposes, and the different risks they pose, the chapter presented a typology of edtech to systematize the complex landscape. The typology differentiated between technologies used to *provide education* and to *learn about education*. The first category was further branched to include technologies that support either educational institutions or teaching and learning activities. Although the latter

could also be seen as a single category, research has shown that popular technologies usually focus on replacing teachers and include minor modifications to support them at the end of the design process, such as dashboards. The different objectives also influence the analysis of necessity and proportionality concerning their impact on children's rights to privacy and data protection.

1064. Finally, the second broader category is related to technologies that seek to learn about how students learn. Although the technologies and data used to power them are often the same as those for supporting students, there is a difference in their purpose. Learning about how students learn is generally a phase of the data analytics process within edtech, and the insights developed therein are fed back into the AI model, influencing the student's own experience while learning. Learning analytics technologies are usually employed to analyze data from longer periods and focus on structure interventions on the algorithm of AI system in general, or even on the curriculum and other elements that may prevent students' progress.

1065. **Chapter 2** explored foundational aspects within edtech and how they interplay with long-standing discussions in education. The first important aspect of interplay involves the participation of private actors in the sector. The rise of neoliberal policies in recent decades has facilitated the marketization of education, either through privatization or commercialization.

1066. *The dynamic between states and private actors has long been established, but the increasing prominence of private sector involvement, particularly in providing digital ICT to schools, has fundamentally altered the very nature of education, i.e., what we understand by it and how it should be realized.* Education is increasingly seen as a private good; students and their families as consumers; and the dynamics of the private sector as the main way to “deliver” it.

1067. *This trend serves as a catalyst for the learnification phenomenon, wherein education is narrowly regarded as synonymous with learning. The emphasis shifts to the transmission of knowledge and skills that individuals should acquire, along with the exploration of efficient methods to achieve it.* This approach sidelines other crucial aspects of a holistic view of education, such as the subjectification and socialization of individuals, as well as education's collective impact and its key role as a foundation for democracy. This broader understanding of education was captured by Paulo Freire's definition of education, as described above, and complemented in Chapter 5 by the aims of education outlined in art. 29, CRC.

1068. *This limited perspective on education further encourages classroom quantification, aligning itself with the educational measurement movement and processes of datafication. Education is seen as something that could and should be modeled and standardized. Beyond concerns about the validity of measurements and what may be overlooked, this mindset shapes curricula and pedagogical methodologies, with targets and indicators being mistaken for the quality of education itself.*

1069. This notion is reinforced by the logic that governs platforms, which increasingly define the landscape of edtech implementation. As an interface that intermediates the user experience and the role of its provider, it helps concretize and interpret abstract processes. They are also progressively integrating aspects of other commercial services, including customization and on-demand features. *While this can potentially enhance engagement, it reflects a belief in learning as a prescriptive process, impacting students' and teachers' autonomy, and naturalizing the processing of extensive amounts of data.*

1070. **Chapter 3** presented the theory of data colonialism as a theoretical and normative lens that guided the discussions in this thesis. The theory refers to an emerging order of appropriation of human life and social relations through data, arguing that our current relationship with personal data could be seen as an extension of historical colonial practices. *The datafication of life leads to the progressive reconfiguration of larger parts of the social domain, as it is increasingly built to generate data. This positions technology companies as privileged providers not only of social solutions but also of social knowledge.*

1071. To better explain their rationale, Couldry and Mejias articulate four main interlinked components that historical colonialism and data colonialism share: appropriation of resources, unequal social and economic relations, uneven global distribution of the benefits of resource appropriation, and ideologies that help us make sense of the new order.

1072. Data are appropriated by the social quantification sector, making use of already existing unequal data relations or creating new ones. These relations are extremely asymmetrical due to (i) the opacity of the operations conducted with personal data, (ii) the powerful overview of the social world that these companies possess as a consequence, and (iii) the fact that they are built on top of historical asymmetries, often as a product of historical colonialism. This intensifies the disparity in value distribution and is justified through specific narratives. Importantly, this theory recognizes that data colonialism affects some people more than others. It means that children, for example, due to their specificities explained in Chapter 4, will have extra layers of

vulnerability compared to adults. Similarly, underprivileged communities will also present additional layers of vulnerability that can profoundly affect their experience with edtech.

1073. Based on this conceptual overview, **Part II** focused on describing and evaluating the current legal framework applicable to children's rights to privacy and to the protection of personal data in the EU and in Brazil. I first discussed why children deserve differential treatment in **Chapter 4**. *The chapter explored their special status as humans in development, which brings them an extra layer of vulnerability.* Specifically within the digital realm, understanding the implications of data processing is already difficult enough for adults. More than a way to enhance fundamental rights, digital technologies are increasingly the gateway for their realization and children have often no choice whether they would like to use them or not for the most different purposes. They are less experienced, can be easily manipulated, and decisions concerning them are generally taken by others on their behalf, and *by having been raised surrounded by technologies, children's lives are increasingly datafied, meaning that they have proportionally larger digital footprints compared to adults.*

1074. The chapter also introduced a risk classification of children's online presence. The matrix included risks to their privacy, broadly understood as encompassing the interpersonal, institutional, and commercial dimensions. It discussed how privacy risks are cross-cutting and extremely connected to other risks children face in the digital realm, reinforcing the need for a holistic children's rights approach. Finally, the chapter underlined the specific implications that surveillance technologies have on children's trust and development, which can hinder their creativity and critical thinking, directly impacting how they learn.

1075. *More importantly, this chapter underscored the need for a comprehensive and nuanced approach to children's presence in the digital environment, which recognizes their distinct characteristics and developmental needs. It acknowledges the transformative potential of edtech in offering opportunities for learning, information access, and developing physical, social, and digital skills. This can help realize several rights enshrined in the CRC, such as the right to education, access to information, play, and freedom of speech. Innovation within the edtech sector should then be fostered to continuously play that role while being integrated into a broader pedagogical strategy based on scientific evidence. At the same time, along with opportunities, edtech also presents risks, as delineated in Part III. Consequently, policymakers, schools, educators, parents, and children must strike a delicate balance, ensuring protective measures while empowering children to grow autonomously.*

1076. **Chapter 5** was dedicated to presenting the CRC and some of its provisions related to the scope of this thesis. It emphasized that discussing the rights to privacy and to the protection of personal data in isolation is not feasible, as they mutually reinforce and impact other rights. For example, the realization of the right to education makes individuals more aware and critical of the issues surrounding them, enabling them to better exercise their rights to privacy and data protection. On the other hand, ensuring the latter is essential for the implementation of quality education, allowing children to feel secure in learning and interacting with educators and fellow students.

1077. First, I presented some provisions considered to be cross-cutting standards that should be used to interpret and implement other articles of the CRC. *The principle of the best interests of the child particularly stands out, as it should be viewed as a fundamental right, interpretative principle, and procedural rule. It also plays an essential role in raising the threshold regarding interferences with children's fundamental rights, serving as a precautionary principle.* These standards also include the right to non-discrimination, the right to be given appropriate direction based on the evolving capacities of the child, and the right to be heard.

1078. Additionally, I have addressed three more substantial provisions: the right to privacy, the right to education, and the right to protection against economic exploitation. The objectives of education delineated in art. 29 of the CRC should consistently guide the advancement of edtech, ensuring it upholds children's privacy from its conception.

1079. *Safeguarding children's right to protection against economic exploitation is paramount within the digital environment and should go beyond the protection against child labor, encompassing any form of exploitation driven by economic and commercial interests. This stance resonates with the concept of data colonialism, which recognizes exploitation within the realm of data commodification. A critical implication of this perspective is that children's data should not be exploited for commercial purposes not aligned with their best interests.* This does not imply a blanket prohibition on procuring edtech or processing data for ancillary activities related to the provided service (such as invoicing). Rather, it means that children's data should not be processed solely for the sake of commercial interests and financial gain, as this would also go against the need to prioritize their rights.

1080. **Chapters 6 and 7** discussed how the GDPR and the LGPD regulate the processing of children's data and how these rules relate to the implementation of edtech by schools. The focus of these chapters was not necessarily on comparing laws, although something inevitable due to

their similarity, but on describing and evaluating their potential, limitations, and gaps to deal with the challenges presented in Part III of the thesis. The current legal frameworks of both jurisdictions already incorporate fundamental rules for safeguarding children's data within edtech. However, there has been limited exploration into the specific purposes for which children's data may be processed, as well as how the mindset of data commodification could serve as the root cause of various risks described in Chapter 8. *While this could certainly be argued to fall within the scope of the right not to be subjected to economic exploitation, it has yet to be translated into enforceable obligations for data controllers beyond the existing prohibition of profiling for targeted advertising purposes in the DSA.*

1081. Despite not being the main focus of this thesis, considering the lack of a final text, the AI Act is also important in the discussion of AI-powered edtech more suitable for the best interests of children. It not only considers certain AI systems deployed in education as high-risk, but also prohibits the use of emotion recognition in this environment.

1082. High-risk systems must comply with various specific obligations, such as those related to data management, cybersecurity, accuracy, and the prevention of bias, which would address many challenges described in Chapter 8. *However, it appears that the AI Act cannot be relied upon as a panacea. Several fundamental questions remain unanswered, including how to align the risk-based approach within an originally product safety legislation with the need to consider values such as human rights, democracy, and the rule of law, as well as the fact that risk assessment is self-assessed, what is problematic due to conflicts of interest.* Despite still being behind in the legislative process and focusing more on the rights of those affected by AI, it is possible to say that similar challenges are going to be faced in the implementation of Bill 2,838 in Brazil.

1083. **Part III** was formulated based on a descriptive, evaluative, and normative approach, aiming to map the challenges posed by data-driven edtech to children's rights to privacy and to the protection of personal data. Given that the majority of data processing activities within edtech involve AI systems, **Chapter 8** initially focused on the overarching risks they present. It began by examining the process of datafication itself and the issues arising from the reduction and abstraction of reality into quantifiable variables. Additionally, it briefly addressed the training of AI systems and highlighted how the substantial amount of data required for their training and operation, along with the issue of repurposing data, already creates tension with the principles of purpose limitation and data minimization in the GDPR and LGPD.

1084. I have also emphasized the concerns surrounding data generation within AI systems and how] inferences drawn therein can be tainted with bias and significantly affect individuals' control over their data. *I have argued that this issue does not seem to be fully addressed by either the GDPR/LGPD or the current text of the AI Act/Bill 2,338. Consequently, there should be a greater focus on the outputs of AI systems and the development of more tools for controlling personal data, such as the right to reasonable inferences.*

1085. Finally, I have also presented the challenges related to decision-making involving algorithms, such as profiling, predictions, and human interpretation of data. Decisions made within edtech have a direct bearing on children's academic performance and their future prospects. *Algorithmic predictions can not only solidify past circumstances, hindering social mobility, but also shape future outcomes as patterns are not merely identified but actively constituted.*

1086. After presenting horizontal challenges related to AI in education, I have also discussed specific ones identified within personalized learning, student monitoring technologies, and learning analytics. Technologies for personalized learning were analyzed as an example of edtech that aims to support students. Despite showing great potential, the evidence of their effectiveness in improving learning is currently weak. On the other hand, the risks already identified are significant. In their current form, this kind of edtech still excessively focus on individual efforts, sidelining social aspects of education, and the aspects that can truly be personalized are limited to the paths that will guide students to the same outcome. Students have a limited ability to define their overall educational goals and, more specifically, the design of the technology and the degree of data processing to which they may be exposed.

1087. Another controversial issue about personalized learning is its internal dynamics and its tendency to amplify what the student is interested in and reduce their contact with the different. Besides being problematic for their learning and development as individuals, it can also affect how the student deals with diversity in society. The reductionist nature of data-driven technologies' architecture can also lead to consider behaviors merely correlated with better academic outcomes being mistakenly identified as their cause and replicated for other students.

1088. Chapter 8 also discussed monitoring and proctoring technologies as examples that directly automate and aim to support teachers' activities. Although the purposes for the use of this kind of technology are usually noble, such as dealing with students' mental health and preventing cheating, they are not necessarily effective and foster a surveilled environment. This

can hinder students from seeking help or expressing their emotions openly, as well as create a chilling effect that affects children's learning and development. The focus on control and mistrust, under the guise of care, can undermine the development of ethical, responsible citizens and perpetuate biases and inequalities, disproportionately impacting more vulnerable groups.

1089. Finally, this chapter described and analyzed technologies used for learning about learning, as explained above. The concept of learning analytics was discussed, as well as their role in leveraging data from students' interactions with the AI model to generate insightful information about their learning process. They are usually employed to analyze data from longer periods and focus on structure interventions on the algorithm used by the AI system, or even on the curriculum and other elements that may prevent students' progress. While learning analytics hold promise and provide valuable insights to enhance learning efficacy and efficiency, the collected data are generally used for purposes that may not necessarily prioritize the best interests of the child.

1090. The rest of Part III was dedicated to understanding the Google Workspace for Education case in the EU and in Brazil in order to gain insights into its functioning, the business model behind it and how it affects children's rights to privacy and to the protection of personal data. *Due to Google's primary role in pushing forward the current prevailing business model of data-driven technologies and its widespread use in European and Brazilian classrooms, I argue that these insights could be extrapolated to other technologies. It helps us not only better understand how to enhance the enforcement activities of the current applicable legal framework, but also assess if further legislation or policies are needed.*

1091. **Chapter 9** focused on describing what Google Workspace for Education is, its main features, and its role in Google's broader business model. I have discussed how, although being considered free and part of the company's initiatives focused on social responsibility, Google Workspace for Education is still tied to Google's commercial interests. The blurred boundaries between core and additional services, with varying levels of data protection; their indirect access to children's data via other edtech; and the use of data for other commercial purposes beyond targeted advertising demonstrate how Google Workspace for Education can be used as a strategic tool within its business model.

1092. **Chapter 10** examined the impacts Google Workspace for Education has had on children's privacy and data protection in two different jurisdictions: the European Union and Brazil. To map the challenges faced within the EU, I have used decisions made by competent

authorities as a filter, taking advantage of their auditing capabilities and comprehensive DPIAs carried out within the scope of some cases. Such information is not available for the Brazilian reality, which prompted the examination of Google Workspace for Education's ToS and Privacy Policies to check their compliance with LGPD whenever possible. This has been complemented by a literature review of studies that have also performed a similar exercise and gathered further data through information requests. We have seen that although both jurisdictions feature very similar data protection laws, they significantly differ in their levels of maturity regarding data protection culture, which directly impacts enforcement activities.

1093. Finally, **Chapter 11** analyzed the data described in Chapter 10 to find convergences, divergences, and gaps not only based on main areas of tension with data protection laws, but also through the lens of data colonialism. *This analysis shows a systematized lack of compliance of schools and Google Workspace for Education with data protection frameworks and sheds light on broader challenges.*

1094. Two main conclusions could be drawn from the Google Workspace for Education case. First, *adequate enforcement of the current legal framework is still needed to safeguard children's rights to privacy and to the protection of personal data.* Within the EU, there is evidently a greater concern regarding the use of edtech, particularly in relation Google Workspace for Education. However, there are also regional disparities that result in national decisions being primarily made by the wealthiest and most powerful countries within the bloc. *In the case of Brazil, the enforcement of the LGPD is still in its early stages, and much still needs to be done to ensure that its rules are followed.*

1095. Second, even in cases where authorities negotiated with Google to align the employment of the edtech with the GDPR, *the business model based on data commodification adopted by Google can be considered, in itself, harmful to children's best interests.* Although their data are not directly used for targeted advertisement within the core services, it is still processed for other commercial purposes. Children are familiarized and nudged to continue using the technology outside the school environment and throughout their lives. *This results in the need to discuss the actual purposes we would like children's data to be processed for and to rethink the epistemologies we currently use to understand the role of data within society.*

1096. We have seen that economic and political capital are essential to achieving even basic compliance with the GDPR. *The social and economic disparities within the EU and between*

the EU and Brazil highlight how profound the influence of the social quantification sector is on countries' digital sovereignty and, consequently, on individual autonomy and democracy.

1097. It highlights that despite the EU's ongoing efforts to implement its data strategy, adding constant pages to its digital rulebook, *it is still necessary to discuss the core essence of digital sovereignty. It prompts us to question whether the policies being implemented genuinely enhance both individual and collective autonomy, or are possibly reinforcing problematic DDBM.* We should also question whether all the EU values are actually being considered, or if innovation and economic development of a few are being prioritized. In light of the Brussels effect, the ramifications of these policies need also to be carefully weighted, justifying global dialogues on digital sovereignty that effectively support individuals and communities beyond the limits of countries, blocs, and companies.

Recommendations and indications for future research

1098. Based on the findings described above, it is possible to outline a few recommendations and suggestions for future research. These are mainly focused on states, the primary duty bearers when it comes to implementing edtech in schools, but some are also directed to technology companies.

1099. States have many roles to play in addressing the concerning scenario depicted throughout the thesis. Considering that the private sector is the main one developing edtech and that innovation requires investment, one of the best ways for states to steer it in the right direction is through public procurement. Public procurement should ideally be seen through the lens of a mission-oriented approach. This includes selecting pathways for the economy and placing the issues that require solution at the core of economic system's design; crafting policies that stimulate investment, innovation, and collaboration among different stakeholders, making sure to involve both businesses and citizens; discussing the type of markets we as a society want; and using instruments to foster the most innovative solutions for addressing specific challenges according to our collective needs and purposes (Mazzucato, 2021).

1100. When it comes to safeguarding children's data, public procurement could serve as a mechanism to choose only the technologies that align with the societal goals we have collectively established. The thesis has demonstrated that this process is most effective when centralized to some extent, enhancing bargaining power with technology companies. It does not necessarily imply that it should only be carried by a single governmental actor but it could be a

collective decision-making process involving various schools or administrative entities. Collaborating interdepartmentally can also boost the full scale of public procurement, enabling the use of a substantially larger budget (Mazzucato, 2021).

1101. If doing it at scale is not possible, states should provide schools with standards to understand and choose among vetted edtech products, as schools are probably not in the best position to evaluate and understand all of their nuances due to a lack of expertise and resources. (Hillman, 2022). A roadmap that can help schools and other administrative entities navigate not only the technological specificities of existing edtech but also existing evidence and the applicable legal framework is an interesting tool to be developed in future research.

1102. As we have seen throughout the thesis, this can be a challenge in cases where the educational budget is insufficient or not prioritized for purchasing technologies and contracting services that are privacy-friendly, such as in Spain or in Brazil. Being free is often the main reason for choosing some technologies. In these cases—always considering the best interest of the child and the legal frameworks described in this thesis—it is possible to envision a path that can assist in decision-making.

1103. The first step that should be applied to any decision by states or schools (whether the product/service is free or not) is to analyze whether the technology is indeed necessary for the specific context. If the desired outcome can be achieved without technology or through applications with simpler algorithms or that require less personal data, these should be prioritized. The availability of technologies should not inevitably lead to their implementation, and a potential “modernization” of education should not be pursued for its own sake. This also includes analyzing their effectiveness, efficiency, and added value more generally (Smuha, 2023b, p. 133), taking into account a holistic analysis of their effects on education and on children’s rights. This could be carried out, for instance, by leveraging CRIAs methodologies. The choice of technology must always be evidence-based and use the best interest of the child as a precautionary principle. Considering all their specificities, children should not be used for experiments of which we do not know the real consequences.

1104. Following this assessment, and considering the actual necessity of the technology for the specific context, a shift in mindset must begin to take place within the public sector. It must begin to see itself as a purchaser oriented towards the public good. This entails understanding the true underpinnings of the technology, including its business model, and recognizing the value it derives when offering its services free of charge. If a company benefits from future

customers despite not receiving direct payment, it means it has an underlining interest in offering the service. The public sector should leverage this dynamic in negotiating more favorable contracts that prioritize the best interests of the child, including opting for technology with privacy-friendly business models. Selling products or providing services to public educational institutions should be regarded as a privilege accompanied by significant responsibility, meaning that edtech companies should adhere to minimum legal and ethical standards (Hillman, 2022).

1105. Apart from procurement, States can also use their resources to directly foster, develop, or improve (core) digital infrastructure in order to make sure they are digitally sovereign and less dependent on external providers. This is aligned with need to transcend data universalism. The discourse around big data and datafication tends to homogenize social-economic and political contexts, overlooking cultural nuances. Viewing technologies as social-technical artifacts prompts an understanding that although opposing homogenization must be global in framing, solutions must be local.

1106. An interesting type of investment is related to using open standards and open-source software, as well as technology that promote privacy, democratic participation and human centrality by design (Herlo; Ullrich; Vladova, 2023). Apart from being less expensive to implement, they provide extra means of auditing not available in proprietary technologies. This also means fostering the development of technology by and for the community which will directly use it based on their needs. An interesting example in this regard is the Brazilian Homeless Worker Movement (Movimento dos Trabalhadores sem Teto – MTST). The movement has an internal group focused on digital technology, which aims not only to empower participants to become self-sovereign in relation to technologies but also to choose and apply technologies that can address the movement's most immediate issues with autonomy and minimal side effects (Grohmann, 2023; Núcleo de Tecnologia do MTST, 2023).

1107. States have also the power and the duty to properly legislate on the issue of edtech and, especially, AIED. This includes not only demanding privacy-friendly design, but also understanding how AI systems affect data control and questioning the sufficiency of the current legal and policy framework to deal with the economic and political structures enabling data commodification. It also encompasses restricting business models that can harm human dignity and human rights, especially concerning the most vulnerable groups. This should particularly consider the social-economic specificities of each state, which can affect the possibilities of enforcement and success of the legislation (Arora, 2019).

1108. Finally, critical thinking and digital literacy of teachers and students should be fostered through training and implementation of specific measures in school curricula. Understanding and properly using digital technologies have become a prerequisite for participation in society and the exercise of fundamental rights. It serves a dual purpose of protecting children's rights, and enabling their participation, equipping them with the necessary tools to navigate the online environment.

1109. Therefore, learning about how technologies function, as well as who the actors and interests behind them are, is essential for nurturing citizens who are critical and engaged in society. This should certainly be seen as a crucial step, but its value is limited if the preceding measures are not taken. As individuals, there is little one can do in the face of the power of certain edtech companies, so the most significant decisions regarding technology and data governance must be made collectively.

1110. When it comes to edtech companies, they should be seen as the ones to bear the primary responsibility for children's data protection. We have seen throughout the thesis, for example, that the design of learning platforms often resembles those of social media, based on maximizing data processing, and the recommendation of content based on what the student has previously engaged with (5Rights Foundation, 2023). We have also seen that edtech industry often markets its products to schools based on unsubstantiated success metrics and insinuating misleading effectiveness rates (American Civil Liberties Union (ACLU), 2023).

1111. These are only a few examples of situations that are deliberate, mostly due to commercial imperatives, and that can cause harm to children's rights. The best interest of the child imposes a duty to adhere to ethical and legal standards to deliver the best learning experience possible to children. Practices that are not aligned with it should be abandoned, recalibrated, or redesigned to meet children's real needs (5Rights Foundation, 2023).

1112. This is the tone given by the USA Federal Trade Commission (FTC) in its most recent Notice of Proposed Rulemaking (NPRM) that proposes changes to the Children's Online Privacy Protection Rule (COPPA Rule). According to the FTC Chair Lina M. Khan, children should be able to play and learn in the digital environment without being tracked by companies that seek to monetize their personal data (Federal Trade Commission (FTC), 2023).

1113. The proposal places affirmative obligations on service providers, shifting the burden historically placed on parents. Some of the changes to the rule proposed by the FTC are directly related to edtech and include a prohibition on commercial use of children's data, including for

the development of different services (Federal Trade Commission (FTC), 2023; Vance; Sexton; Kalpos, 2023). Others are more general such as a prohibition against conditioning a child's participation on collection of personal information, limits on nudging kids to stay online and the requirement of a separate opt-in for targeted advertising.

1114. As a society, including state agents, businesses, families we must approach the topic discussed in this thesis with the gravity it warrants. The success of future generations hinges on the actions taken by today's adults on their behalf, and we have yet to fully grasp the breadth of the long-term effects that data-driven digital ICT will have on children's rights. More significantly, today's children will inhabit an increasingly interconnected world dominated by digital technologies, particularly AI. In this landscape, the boundaries between human-created and machine-created becomes increasingly blurred, as well as what is true or false. The most important decisions about children's lives will very often be made based on what data say about them.

1115. What we allow to be applied and developed today will shape how younger generations navigate the complex problems of the world we are entrusting to them. We must take charge of technological development to ensure it is evidence-based and human-centric. Instead of us becoming dependent on and serving technology (and technology companies), technology should serve the purposes we have collectively defined.

REFERENCES

- 5RIGHTS FOUNDATION. **Disrupted Childhood: The cost of persuasive design**. [S. l.: s. n.], 2023. Available at: <https://5rightsfoundation.com/uploads/Disrupted-Childhood-2023-v2.pdf>. Accessed on: 26 dec. 2023.
- 5RIGHTS FOUNDATION. **Pathways: How digital design puts children at risk**. [S. l.: s. n.], 2021. Available at: <https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf>. Accessed on: 8 jun. 2023.
- AEPD. **Resolución de Procedimiento Sancionador. Expediente N.º EXP202102527**. [S. l.: s. n.], 2023a. Available at: <https://www.aepd.es/documento/ps-00176-2022.pdf>. Accessed on: 6 dec. 2023.
- AEPD. **Resolución de Procedimiento Sancionador. Expediente N.º EXP202104450**. [S. l.: s. n.], 2023b.
- AEPD. **Resolución de Recurso de Reposición. Expediente N.º EXP202104450**. [S. l.: s. n.], 2023c. Available at: <https://www.aepd.es/documento/reposicion-ps-00334-2022.pdf>. Accessed on: 6 dec. 2023.
- AGÊNCIA SENADO. Política Nacional de Educação Digital é sancionada com vetos. **Senado Notícias**, [s. l.], 12 jan. 2023. Available at: <https://www12.senado.leg.br/noticias/materias/2023/01/12/politica-nacional-de-educacao-digital-e-sancionada-com-vetos#:~:text=O%20presidente%20Luiz%20In%C3%A1cio%20Lula,programa%C3%A7%C3%A3o%20e%20rob%C3%B3tica%20nas%20escolas>. Accessed on: 25 oct. 2023.
- AGUIAR JÚNIOR, Ruy Rosado de. **Jornadas de Direito Civil I, III, IV e V: Enunciados Aprovados**. Brasília: [s. n.], 2012. Available at: <https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/EnunciadosAprovados-Jornadas-1345.pdf>. Accessed on: 9 oct. 2023.
- ALLEN, Simon. How A Culture Of Listening Can Drive Digital Transformation. **Forbes**, [s. l.], 9 sep. 2022. Available at: <https://www.forbes.com/sites/forbesbusinesscouncil/2022/09/09/how-a-culture-of-listening-can-drive-digital-transformation/>. Accessed on: 30 jul. 2023.
- ALSTON, Philip. **Extreme poverty and human rights. Note by the Secretary-General. A/74/493**. [S. l.: s. n.], 2019. Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/312/13/PDF/N1931213.pdf?OpenElement>. Accessed on: 1 jul. 2023.
- AMERICAN CIVIL LIBERTIES UNION (ACLU). **Digital Dystopia: The Danger in Buying What the EdTech Surveillance Industry is Selling**. [S. l.: s. n.], 2023. Available at: <https://www.aclu.org/publications/digital-dystopia-the-danger-in-buying-what-the-edtech-surveillance-industry-is-selling>. Accessed on: 25 dec. 2023.

AMIEL, Tel *et al.* Os modos de adesão e a abrangência do capitalismo de vigilância na educação brasileira. **Perspectiva**, [s. l.], v. 39, n. 3, p. 1–22, 2021.

AMIEL, Tel; GONSALES, Priscila; SEBRIAM, Debora. Recursos Educacionais Abertos no Brasil: 10 anos de ativismo. **Em Rede: Revista de Educação à Distância**, [s. l.], v. 5, n. 2, 2018. Available at: <https://www.aunirede.org.br/revista/index.php/emrede/article/view/346/326>. Accessed on: 25 oct. 2023.

ANPD. **Estudo Preliminar: Hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes**. 2022a. Available at: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/estudo-preliminar-tratamento-de-dados-crianca-e-adolescente.pdf>. Accessed on: 5 oct. 2023.

ANPD. **Glossário de Proteção de Dados Pessoais e Privacidade**. 2024a Available at: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/glossario-anpd-protecao-de-dados-pessoais-e-privacidade.pdf>. Accessed on: 5 Feb. 2024.

ANPD. **Guia Orientativo. Hipóteses Legais de Tratamento de Dados Pessoais: Legítimo Interesse**. 2024b. Available at: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_legitimo_interesse.pdf. Accessed on: 5 feb. 2024.

ANPD. **Perguntas e Respostas sobre o Relatório de Impacto à Proteção de Dados Pessoais**. [S. l.], 2023. Available at: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Accessed on: 8 oct. 2023.

ANPD. Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. **Diário Oficial da União, Edição 20, Seção 1**: Brazil, n. Resolução CD/ANPD Nº 2, p. 6, 27 jan. 2022b. Available at: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019#wrapper>. Accessed on: 8 oct. 2023.

AP. **Advies Autoriteit Persoonsgegevens (AP) aan SURF en SIVON inzake Google G Suite for Education**. [S. l.: s. n.], 2021a. Available at: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z10202&did=2021D22378. Accessed on: 27 sep. 2023.

AP. **Borging privacy in het onderwijs bij Google producte**. [S. l.: s. n.], 2023. Available at: https://www.autoriteitpersoonsgegevens.nl/uploads/imported/brief_ap_privacy_in_het_onderwijs_bij_google-producten.pdf. Accessed on: 27 sep. 2023.

AP. **Brief van de Autoriteit Persoonsgegevens aan de minister van Onderwijs Cultuur en Wetenschap over borging privacy in het onderwijs en de inzet van Google G Suite for Education**. [S. l.: s. n.], 2021b.

AP. **Brief van de Autoriteit Persoonsgegevens aan de minister voor Basis- en Voortgezet Onderwijs en Media over borging privacy in het onderwijs en de inzet van Google G Suite**

for Education. [S. l.: s. n.], 2021c. Available at: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z10202&did=2021D22378. Accessed on: 27 sep. 2023.

ARORA, Payal. General Data Protection Regulation-A Global Standard? Privacy Futures, Digital Activism, and Surveillance Cultures in the Global South. **Surveillance & Society**, [s. l.], v. 17, n. 5, p. 717–725, 2019.

ARORA, Payal. The Bottom of the Data Pyramid: Big Data and the Global South. **International Journal of Communication**, [s. l.], v. 10, p. 1681–1699, 2016. Available at: <https://ijoc.org/index.php/ijoc/article/view/4297/1616>. Accessed on: 20 jun. 2023.

ASSEMBLÉE NATIONALE. **16ème législature. Question N° 971 de M. Philippe Latombe (Démocrate (MoDem et Indépendants) - Vendée) Question écrite.** [S. l.: s. n.], 2022a. Available at: <https://questions.assemblee-nationale.fr/q16/16-971QE.htm>. Accessed on: 30 sep. 2023.

ASSEMBLÉE NATIONALE. **Numérique. Gratuité d’Office 365.** [S. l.: s. n.], 2022b. Available at: https://questions.assemblee-nationale.fr/static/16/questions/jo/jo_anq_202234.pdf. Accessed on: 30 sep. 2023.

ATABEY, Ayca. Balancing interests in EdTech: When is the lawful basis of “legitimate interests” justified? **The Digital Futures Commission, 5Rights Foundation**, [s. l.], 20 sep. 2021.

AUSLOOS, Jef. Balancing in the GDPR: legitimate interests v. right to object. **Centre for IT and IP Law Blog**, Leuven, 28 fev. 2017. Available at: <https://www.law.kuleuven.be/citip/blog/balancing-in-the-gdpr-legitimate-interests-v-right-to-object/>. Accessed on: 20 fev. 2024.

BÄCKE, Maria. Resisting Commodification: Subverting the Power of the Global Tech Companies. **Bandung**, [s. l.], v. 9, n. 1–2, p. 49–79, 2022.

BAKER, Ryan S. Artificial Intelligence in education: Bringing it all together. *In*: OECD (org.). **OECD Digital Education Outlook 2021: Pushing the Frontiers with Artificial Intelligence, Blockchain and Robots**,. Paris: OECD Publishing, 2021. p. 43–54. Available at: <https://doi.org/10.1787/589b283f-en>. Accessed on: 12 nov. 2023.

BANK, Max *et al.* **The Lobby Network: Big Tech’s Web of Influence in the EU.** [S. l.: s. n.], 2021. Available at: <https://corporateeurope.org/sites/default/files/2021-08/The%20lobby%20network%20-%20Big%20Tech%27s%20web%20of%20influence%20in%20the%20EU.pdf>. Accessed on: 27 sep. 2023.

BARASSI, Veronica. **CHILD | DATA | CITIZEN.** [S. l.]: MIT Press, 2020.

BAROCAS, Solon; SELBST, Andrew D. Big Data’s Disparate Impact. **California Law Review**, [s. l.], v. 104, n. 3, p. 671–732, 2016. Available at: <http://dx.doi.org/10.15779/Z38BG31>.

BARRET, Lindsey *et al.* **The Case for Better Governance of Children's Data: A Manifesto.** [S. l.: s. n.], 2021. Available at: <https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance>. Accessed on: 9 oct. 2023.

BATES, A. W. **Teaching in a Digital Age - Second Edition.** [S. l.]: Tony Bates Associates, 2019. Available at: <https://pressbooks.bccampus.ca/teachinginadigitalagev2/>.

BEDINGFIELD, Will. Everything that went wrong with the botched A-Levels algorithm. **Wired**, [s. l.], 19 aug. 2020. Available at: <https://www.wired.co.uk/article/alevel-exam-algorithm>. Accessed on: 4 mai 2023.

BEIJING CONSENSUS ON ARTIFICIAL INTELLIGENCE AND EDUCATION. . [S. l.: s. n.], 2019. Available at: <https://unesdoc.unesco.org/ark:/48223/pf0000368303>. Accessed on: 17 dec. 2023.

BERTRAND, Melanie; MARCH, Julie. How data-driven reform can drive deficit thinking. **Phi Delta Kappan**, [s. l.], v. 102, n. 8, p. 35–39, 2021.

BERTRAND, Melanie; MARSH, Julie A. Teachers' Sensemaking of Data and Implications for Equity. **American Educational Research Journal**, [s. l.], v. 52, n. 5, p. 861–893, 2015.

BESSON, Samantha; KLEBER, Eleonor. Article 2: The Right to Non-Discrimination. In: TOBIN, John; ALSTON, Philip (org.). **The UN Convention on the Rights of the Child: A Commentary.** [S. l.]: Oxford University Press, 2019. p. 41–72. Available at: <http://www>.

BIESTA, Gert. Against learning: Reclaiming a language for education in an age of learning. **Nordik Pedagogik**, [s. l.], v. 25, p. 54–66, 2005. Available at: <http://www.learndirect.co.uk/personal>;

BIESTA, Gert. **Beyond Learning: Democratic Education for Human Future.** [S. l.]: Routledge, 2016a.

BIESTA, Gert. **Good Education in an Age of Measurement: Ethics, Politics, Democracy.** New York: Routledge, 2010.

BIESTA, Gert. **The Beautiful Risk of education.** [S. l.]: Routledge, 2016b.

BINDER, Krisztina. **Progress on the European Commission's 2021-2027 digital education action plan.** [S. l.: s. n.], 2023. Available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/745689/EPRS_BRI\(2023\)745689_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/745689/EPRS_BRI(2023)745689_EN.pdf). Accessed on: 22 oct. 2023.

BIONI, Bruno; GARROTE, Marina; GUEDES, Paula. **Temas Centrais na Regulação de IA: o local, regional e o global na busca da interoperabilidade regulatória.** São Paulo: [s. n.], 2023. Available at: https://www.dataprivacybr.org/wp-content/uploads/2023/12/dataprivacy_nota-tecnica-temas-regulatorios.pdf. Accessed on: 19 dec. 2023.

BONAMIGO, Samuel. Our commitment to the privacy and security of Google Workspace customer data. **Google Cloud Blog**, [s. l.], 2 mar. 2021. Available at: <https://cloud.google.com/blog/topics/inside-google-cloud/our-commitment-to-the-privacy-and-security-of-google-workspace-customer-data>. Accessed on: 27 sep. 2023.

BORNE, Élisabeth. **Actualisation de la doctrine d'utilisation de l'informatique en nuage par l'État (« cloud au centre »)**. [S. l.], 2023. Available at: https://www.legifrance.gouv.fr/circulaire/id/45446?fonds=CIRC&page=1&pageSize=10&query=cloud&searchField=ALL&searchType=ALL&tab_selection=all&typePagination=DEFAULT. Accessed on: 27 sep. 2023.

BOU, Bram. Protecting Students with Google Apps for Education. **Google Cloud Official Blog**, [s. l.], 30 apr. 2014. Available at: <https://cloud.googleblog.com/2014/04/protecting-students-with-google-apps.html>. Accessed on: 10 aug. 2023.

BRADFORD, Anu. **The Brussels effect : how the European Union rules the world**. Oxford: Oxford University Press, 2020.

BRASIL. **Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências**. Brazil: 9 jul. 2019. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/113853.htm. Accessed on: 17 nov. 2023.

BRASIL. **Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Justiça e Segurança Pública e remaneja cargos em comissão e funções de confiança**. Brazil: 1 jan. 2023a. Available at: http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11348.htm. Accessed on: 17 nov. 2023.

BRASIL. **Código Civil (CC)**. Brazil: 10 jan. 2022a. Available at: https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm. Accessed on: 17 nov. 2023.

BRASIL. **Código de Defesa do Consumidor (CDC)**. Brazil: 11 sep. 1990. Available at: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Accessed on: 17 nov. 2023.

BRASIL. **Constituição da República Federativa do Brasil (CRFB)**. Brazil: 5 oct. 1988. Available at: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Accessed on: 17 nov. 2023.

BRASIL. **Estabelece normas educacionais excepcionais a serem adotadas durante o estado de calamidade pública reconhecido pelo Decreto Legislativo nº 6, de 20 de março de 2020; e altera a Lei nº 11.947, de 16 de junho de 2009**. Brazil: 18 aug. 2020. Available at: <https://www.in.gov.br/en/web/dou/-/lei-n-14.040-de-18-de-agosto-de-2020-272981525>. Accessed on: 17 nov. 2023.

BRASIL. **Estabelece o regime jurídico das parcerias entre a administração pública e as organizações da sociedade civil, em regime de mútua cooperação, para a consecução de**

finalidades de interesse público e recíproco, mediante a execução de atividades ou de projetos previamente estabelecidos em planos de trabalho inseridos em termos de colaboração, em termos de fomento ou em acordos de cooperação; define diretrizes para a política de fomento, de colaboração e de cooperação com organizações da sociedade civil; e altera as Leis nºs 8.429, de 2 de junho de 1992, e 9.790, de 23 de março de 1999. 31 jul. 2014. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/113019.htm. Accessed on: 17 nov. 2023.

BRASIL. Institui o Sistema Nacional para a Transformação Digital e estabelece a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital. Brazil: 21 mar. 2018a. Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9319.htm. Accessed on: 17 nov. 2023.

BRASIL. Lei de Acesso à Informação (LAI). Brazil: 18 nov. 2011a. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm. Accessed on: 17 nov. 2023.

BRASIL. Lei de Interceptação Telefônica. Brazil: 24 jul. 1996. Available at: http://www.planalto.gov.br/ccivil_03/leis/19296.htm. Accessed on: 17 nov. 2023.

BRASIL. Lei de Licitações e Contratos Administrativos. Brazil. 1 apr. 2021. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/114133.htm. Accessed on: 1 jan. 2024.

BRASIL. Lei do Cadastro Positivo. Brazil: 9 jun. 2011b. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112414.htm. Accessed on: 17 nov. 2023.

BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). Brazil: 14 aug. 2018b. Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Accessed on: 17 nov. 2023.

BRASIL. Marco Civil da Internet (MCI). Brazil: 23 apr. 2014. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Accessed on: 17 nov. 2023.

BRASIL. Política Nacional da Educação Digital (PNED). 11 jan. 2023b. Available at: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Lei/L14533.htm#:~:text=LEI%20N%C2%BA%2014.533%2C%20DE%2011%20DE%20JANEIRO%20DE%202023&text=Institui%20a%20Pol%C3%ADtica%20Nacional%20de,30%20de%20outubro%20de%202003. Accessed on: 17 nov. 2023.

BRASIL. Projeto de Lei Nº 2338, de 2023, Dispõe sobre o uso da Inteligência Artificial. Brazil: 2023c. Available at: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1701182930272&disposition=inline>. Accessed on: 19 dec. 2023.

BRASIL. **Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis nºs 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº 13.853, de 8 de julho de 2019.** 25 oct. 2022b. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/114460.htm. Accessed on: 17 nov. 2023.

BRAUN, Anette *et al.* **Rethinking education in the digital age.** [S. l.: s. n.], 2020. Available at: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641528/EPRS_STU\(2020\)641528_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641528/EPRS_STU(2020)641528_EN.pdf). Accessed on: 30 jul. 2023.

BRAZILIAN NETWORK INFORMATION CENTER. **2022 ICT in Education. Survey on the Use of Information and Communication Technologies in Brazilian Schools.** São Paulo: [s. n.], 2023. Available at: https://cetic.br/media/docs/publicacoes/2/20231122132216/tic_educacao_2022_livro_completo.pdf. Accessed on: 11 dec. 2023.

BRAZILIAN NETWORK INFORMATION CENTER. **ICT in Education 2020: Survey on the Use of Information and Communication Technologies in Brazilian Schools.** [S. l.: s. n.], 2021. Available at: https://cetic.br/media/docs/publicacoes/2/20211124200326/tic_educacao_2020_livro_eletronico.pdf. Accessed on: 1 nov. 2023.

BRIGGS, S. **The evolution of Learning Technologies.** [S. l.], 2014. Available at: <https://www.opencolleges.edu.au/informed/features/the-evolution-of-learning-technology/>. Accessed on: 11 mar. 2023.

BRIN, Sergey; PAGE, Lawrence. **The anatomy of a large-scale hypertextual Web search engine.** *Computer Networks and ISDN Systems*. Stanford: [s. n.], 1998. Available at: <http://infolab.stanford.edu/pub/papers/google.pdf>. Accessed on: 21 jul. 2023.

BRINKMEYER, Holger. **LfdI Nordrhein-Westfalen gibt Update zum Einsatz von Microsoft 365 in Schulen. Datenschutz Notizen,** [s. l.], 11 jul. 2023. Available at: <https://www.datenschutz-notizen.de/lfdi-nordrhein-westfalen-gibt-update-zum-einsatz-von-microsoft-365-in-schulen-1043574/>. Accessed on: 27 sep. 2023.

BROWNLOW, Josh *et al.* **Data and Analytics-Data-Driven Business Models: A Blueprint for Innovation.** [S. l.: s. n.], 2015. Available at: <https://cambridgeservicealliance.eng.cam.ac.uk/system/files/documents/2015MarchPaperTheDDBMInnovationBlueprint.pdf>. Accessed on: 21 jul. 2023.

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI). **SiSyPHuS Win10: Telemetry in Windows 10.** [S. l.], 2018. Available at: https://www.bsi.bund.de/EN/Service-Navi/Publicationen/Studien/SiSyPHuS_Win10/AP4/SiSyPHuS_AP4_node.html. Accessed on: 27 sep. 2023.

BYGRAVE, Lee A. Article 4(4). profiling. *In*: KUNER, Christopher *et al.* (org.). **The EU General Data Protection Regulation (GDPR): A Commentary**. [S. l.]: Oxford University Press, 2020a. p. 127–131.

BYGRAVE, Lee A. Article 22. Automated individual decision- making, including profiling. *In*: KUNER, Christopher *et al.* (org.). **The EU General Data Protection Regulation: A Commentary**. [S. l.]: Oxford University Press, 2020b. p. 522–542.

CALZATI, Stefano. Decolonising “Data Colonialism” Propositions for Investigating the Realpolitik of Today’s Networked Ecology. **Television and New Media**, [s. l.], v. 22, n. 8, p. 914–929, 2021.

CANNATACI, Joseph A. **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**. [S. l.: s. n.], 2021. Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/015/65/PDF/G2101565.pdf?OpenElement>. Accessed on: 16 jul. 2023.

CARDONA, Miguel A; RODRÍGUEZ, Roberto J; ISHMAEL, Kristina. **Artificial Intelligence and the Future of Teaching and Learning - Insights and Recommendations**. Washington: [s. n.], 2023. Available at: <https://www2.ed.gov/documents/ai-report/ai-report.pdf>. Accessed on: 29 mai 2023.

CARR, John. The children’s privacy debacle – Part 3. **Desiderata: Technology explained**, [s. l.], 6 jan. 2016. Available at: <https://johncarr.blog/2016/01/06/the-childrens-privacy-debacle-part-3/>. Accessed on: 14 jul. 2023.

CASSIDY, Arlette. Age Appropriate. *In*: VOLKMAR, F. R. (org.). **Encyclopedia of Autism Spectrum Disorders**. New York: Springer, 2013.

CENTER FOR DEMOCRACY & TECHNOLOGY (CDT). **Generative AI Systems in Education — Uses and Misuses**. [S. l.: s. n.], 2023. Available at: <https://cdt.org/wp-content/uploads/2023/03/2023-03-15-CDT-Civic-Tech-Generative-AI-issue-brief-final.pdf>. Accessed on: 27 jul. 2023.

CENTER FOR DEMOCRACY & TECHNOLOGY (CDT). **The Chilling Effect of Student Monitoring: Disproportionate Impacts and Mental Health Risks**. [S. l.: s. n.], 2022. Available at: <https://cdt.org/insights/the-chilling-effect-of-student-monitoring-disproportionate-impacts-and-mental-health-risks/>. Accessed on: 8 mai 2023.

CHAKROUN, Borhene *et al.* **Minding the data: Protecting learners’ privacy and security**. Paris: [s. n.], 2022. Available at: <http://www.unesco.org/open-access/terms-> .

CHAUDHARY, Monica. Involvement of Children in the Family Buying: A Review. **Pacific Business Review International**, [s. l.], v. 8, p. 54–62, 2016. Available at: http://www.pbr.co.in/2016/2016_month/May/8.pdf. Accessed on: 2 aug. 2023.

CHENG, Hoi Wai Jackie. **Economic properties of data and the monopolistic tendencies of data economy: policies to limit an Orwellian possibility**. [S. l.: s. n.], 2020. Available at:

<https://www.un.org/en/desa/economic-properties-data-and-monopolistic-tendencies-data-economy-policies-limit>. Accessed on: 18 jun. 2023.

CHIRCOP, Denise. **The European Education Area and the 2030 strategic framework for education and training**. [S. l.: s. n.], 2021. Available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690630/EPRS_BRI\(2021\)690630_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690630/EPRS_BRI(2021)690630_EN.pdf). Accessed on: 22 oct. 2023.

COBBE, Jennifer; SINGH, Jatinder. Artificial intelligence as a service: Legal responsibilities, liabilities, and policy challenges. **Computer Law & Security Review**, [s. l.], v. 42, p. 105573, 2021. <https://doi.org/10.1016/j.clsr.2021.105573>.

COE. **Children's data protection in an education setting. Guidelines. Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data. Convention 108**. [S. l.: s. n.], 2021. Available at: <https://edoc.coe.int/en/children-and-the-internet/9620-childrens-data-protection-in-an-education-setting-guidelines.html>. Accessed on: 9 jul. 2023.

COHEN, Julie E. **Between Truth and Power: The Legal Constructions of Informational Capitalism**. [S. l.]: Oxford University Press, 2019.

COLLINS, Sara *et al.* **The Privacy and Equity Implications of Using Self-Harm Monitoring Technologies: Recommendations for Schools**. [S. l.: s. n.], 2021. Available at: <https://studentprivacycompass.org/resource/self-harm-monitoring/>. Accessed on: 23 mai 2023.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL). **La CNIL appelle à des évolutions dans l'utilisation des outils collaboratifs états-uniens pour l'enseignement supérieur et la recherche**. [S. l.], 2021. Available at: <https://www.cnil.fr/fr/la-cnil-appelle-evolutions-dans-utilisation-outils-collaboratifs-etatsuniens-enseignement-superieur-recherche>. Accessed on: 27 sep. 2023.

COMMITTEE ON ECONOMIC SOCIAL AND CULTURAL RIGHTS. **CESCR General Comment No. 13: The Right to Education (Art. 13)**. [S. l.: s. n.], 1999a.

COMMITTEE ON ECONOMIC SOCIAL AND CULTURAL RIGHTS. **General comment No. 11: Plans of Action for Primary Education (Art. 14)**. [S. l.: s. n.], 1999b. Available at: <https://www.refworld.org/docid/4538838c0.html>. Accessed on: 11 jul. 2023.

COMMITTEE ON THE RIGHTS OF THE CHILD. **General Comment No. 1 (2001). Article 29(1): The aims of education**. [S. l.: s. n.], 2001. Available at: <https://www.refworld.org/docid/4538834d2.html>. Accessed on: 11 jul. 2023.

COMMITTEE ON THE RIGHTS OF THE CHILD. **General Comment No. 5 (2003). General measures of implementation of the Convention on the Rights of the Child (arts. 4, 42 and 44, para. 6). CRC/GC/2003/5**. [S. l.: s. n.], 2003. Available at: <https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsiQql8gX5Zxh0cQqSRzx6Zd2%2FQRsDnCTcaruSeZhPr2vUevjbn6t6GSilfheVp%2Bj5HTLU2Ub%2FPZZtQWn0jExFVnWuhiBbqgAj0dWBoFGbK0c>. Accessed on: 8 jul. 2023.

COMMITTEE ON THE RIGHTS OF THE CHILD. **General Comment No. 12 (2009). The right of the child to be heard. CRC/C/GC/12.** [S. l.: s. n.], 2009.

COMMITTEE ON THE RIGHTS OF THE CHILD. **General comment No. 13 (2011). The right of the child to freedom from all forms of violence. CRC/C/GC/13.** [S. l.: s. n.], 2011. Available at: https://www2.ohchr.org/english/bodies/crc/docs/crc.c.gc.13_en.pdf. Accessed on: 23 jun. 2023.

COMMITTEE ON THE RIGHTS OF THE CHILD. **General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (art. 3, para. 1). CRC/C/GC/14.** [S. l.: s. n.], 2013a.

COMMITTEE ON THE RIGHTS OF THE CHILD. **General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights. CRC/C/GC/16.** [S. l.: s. n.], 2013b. Available at: <https://www2.ohchr.org/english/bodies/crc/docs/crc.c.gc.16.pdf>. Accessed on: 8 jul. 2023.

COMMITTEE ON THE RIGHTS OF THE CHILD. **General comment No. 20 (2016) on the implementation of the rights of the child during adolescence. CRC/C/GC/20.** [S. l.: s. n.], 2016. Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/404/44/PDF/G1640444.pdf?OpenElement>. Accessed on: 9 jul. 2023.

COMMITTEE ON THE RIGHTS OF THE CHILD. **General comment No. 25 (2021) on children's rights in relation to the digital environment. CRC/C/GC/25.** [S. l.: s. n.], 2021. Available at: <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>. Accessed on: 26 jun. 2023.

COMPUTER-BASED LEARNING. [S. l.], 2009. Available at: https://edutechwiki.unige.ch/en/Computer-based_learning. Accessed on: 11 mar. 2023.

COMPUTER-BASED TRAINING. [S. l.], 2009. Available at: https://edutechwiki.unige.ch/en/Computer-based_training. Accessed on: 11 mar. 2023.

CONSED. NOVA ESCOLA, com apoio da Fundação Lemann e do Google.org, lança primeiros planos de aula alinhados à BNCC, 2018. Available at: <https://www.consed.org.br/noticia/nova-escola-com-apoio-da-fundacao-lemann-e-do-google-org-lanca-primeiros-planos-de-aula-alinhados-a-bncc>. Accessed on: 11 dec. 2023.

CONSED. Sobre o Consed, [s. d.]. Available at: <https://www.consed.org.br/conteudos/sobre-o-consed>. Accessed on: 11 dec. 2023.

CONSELHO DA JUSTIÇA FEDERAL. **Jornadas de Direito Civil Enunciados Aprovados.** [S. l.], [s. d.].

CORCORAN, Betsy. A Brief History of (Edtech) Time. **Texas Education Review**, [s. l.], v. 1, p. 104–118, 2013.

CORPORATE EUROPE OBSERVATORY. **How the Commission outsourced its merger policy to Google's best friend.** [S. l.], 2023. Available at: <https://corporateeurope.org/en/2023/04/how-commission-outsourced-its-merger-policy-google-best-friend>. Accessed on: 14 sep. 2023.

CORTADA, James W. **Before the computer : IBM, NCR, Burroughs, and Remington Rand and the industry they created, 1865-1956.** [S. l.]: Princeton University Press, 1993.

CORTESI, Sandra *et al.* **Youth and Extended Reality: An Initial Exploration of Augmented, Virtual, and Mixed Realities.** [S. l.: s. n.], 2021. Available at: <https://cyber.harvard.edu/publication/2021/youth-extended-reality>. Accessed on: 30 jul. 2023.

COTHRAN, Ann; MASON, George E. The Typewriter: Time-Tested Tool for Teaching Reading and Writing. **The Elementary School Journal**, [s. l.], v. 78, n. 3, p. 170–173, 1978. Available at: <https://www.jstor.org/stable/1001415>. Accessed on: 15 mai 2023.

COULDRY, Nick; DIJCK, José van. Researching Social Media as if the Social Mattered. **Social Media and Society**, [s. l.], v. 1, n. 2, 2015.

COULDRY, Nick; MEJIAS, Ulises A. **The Costs of Connection: How Data is Colonising Human Life and Appropriating it for Capitalism.** Stanford: Stanford University Press, 2019.

COULDRY, Nick; MEJIAS, Ulises Ali. The decolonial turn in data and technology research: what is at stake and where is it heading?. **Information Communication and Society**, [s. l.], v. 26, n. 4, p. 786–802, 2023.

COUNCIL OF THE EUROPEAN UNION. **Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world.** [S. l.], 2023a. Available at: <https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/>. Accessed on: 18 dec. 2023.

COUNCIL OF THE EUROPEAN UNION. **Council Recommendation of 22 May 2018 on key competences for lifelong learning. ST/9009/2018/INIT.** [S. l.: s. n.], 2018a. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AC%3A2018%3A189%3ATOC&uri=uriserv%3AOJ.C_.2018.189.01.0001.01.ENG. Accessed on: 22 oct. 2023.

COUNCIL OF THE EUROPEAN UNION. **Council Recommendation of 22 May 2018 on promoting common values, inclusive education, and the European dimension of teaching. ST/9010/2018/INIT.** [S. l.: s. n.], 2018b. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018H0607%2801%29>. Accessed on: 22 oct. 2023.

COUNCIL OF THE EUROPEAN UNION. **Council Resolution on a strategic framework for European cooperation in education and training towards the European Education Area and beyond (2021-2030) 2021/C 66/01.** [S. l.: s. n.], 2021a. Available at: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32021G0226%2801%29>. Accessed on: 22 oct. 2023.

COUNCIL OF THE EUROPEAN UNION. **Council Resolution on the governance structure of the strategic framework for European cooperation in education and training towards the European Education Area and beyond (2021-2030) 2021/C 497/01. ST/14487/2021/INIT.** [S. l.: s. n.], 2021b. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021G1210%2801%29>. Accessed on: 22 oct. 2023.

COUNCIL OF THE EUROPEAN UNION. **Press conference following the trilogue on artificial intelligence.** [S. l.], 2023b. Available at: <https://video.consilium.europa.eu/event/en/27283>. Accessed on: 18 dec. 2023.

COUNCIL OF THE EUROPEAN UNION. **Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Analysis of the final compromise text with a view to agreement.** Brussels, 2024. Available at: <https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf>. Accessed on: 30 jan. 2024.

COURSERA. **2021 Impact Report. Serving the world through learning.** [S. l.: s. n.], 2021. Available at: <https://aboct.coursera.org/press/wp-content/uploads/2021/11/2021-Coursera-Impact-Report.pdf>. Accessed on: 12 nov. 2023.

COURTIS, Christian; TOBIN, John. Article 28. The Right to Education. In: TOBIN, John (org.). **The UN Convention on the Rights of the Child: A Commentary.** Oxford: Oxford University Press, 2019. p. 1056–115.

COWAN, Leah; ARBOINE, Niellah; ALEMORU, Kemi. **For black students, badly-predicted grades are the tip of the iceberg.** [S. l.], 2020. Available at: <https://gal-dem.com/for-black-students-badly-predicted-grades-are-the-tip-of-the-iceberg/>. Accessed on: 5 mai 2023.

CRANDALL, Marc. Helping European education providers navigate privacy assessments. **Google Cloud Blog**, [s. l.], 18 aug. 2022a. Available at: <https://cloud.google.com/blog/products/identity-security/helping-european-education-providers-navigate-privacy-assessments>. Accessed on: 27 sep. 2023.

CRANDALL, Marc. Introducing new commitments on the processing of service data for our cloud customers. **Google Cloud Blog**, [s. l.], 17 jun. 2022b. Available at: <https://cloud.google.com/blog/products/identity-security/introducing-new-commitments-on-the-processing-of-service-data-for-our-cloud-customers>. Accessed on: 27 sep. 2023.

CRUZ, Leonardo Ribeiro da; VENTURINI, Jamila Rodrigues. Neoliberalismo e crise: o avanço silencioso do capitalismo de vigilância na educação brasileira durante a pandemia da Covid-19. **Revista Brasileira de Informática na Educação**, [s. l.], v. 28, p. 1060–1085, 2020.

CYNDECKA, Malgorzata Agnieszka. A dystopian story about COVID-19, Artificial Intelligence setting grades and the GDPR. **EFTA-Studies.org**, [s. l.], 5 sep. 2020. Available at: <https://www.efta-studies.org/post/a-dystopian-story-about-covid-19-artificial-intelligence-setting-grades-and-the-gdpr>. Accessed on: 17 oct. 2023.

CZERNIEWICZ, L. Educational technology - mapping the terrain with Bernstein as cartographer. **Journal of Computer Assisted Learning**, [s. l.], v. 26, n. 6, p. 523–534, 2010.

DAMANI, Kalifa; MITCHELL, Joel. **Rapid Evidence Review: Radio**. [S. l.: s. n.], 2020. Available at: http://edtechhub.org/wp-content/uploads/2020/09/Rapid-Evidence-Review_Radio-1.pdf. Accessed on: 24 jul. 2023.

DARK, Martha. UK: Legal action threatened over algorithm used to grade teenagers' exams. **Statewatch**, [s. l.], 12 aug. 2020. Available at: <https://www.statewatch.org/news/2020/august/uk-legal-action-threatened-over-algorithm-used-to-grade-teenagers-exams/>. Accessed on: 17 oct. 2023.

DATA MINING OF SCHOOL KIDS. direção: Jose Ferreira. [S. l.]: Knewton Education Datapalooza, 2012. Available at: <https://www.youtube.com/watch?v=qIbMLVJi4qc&t=0s>. Accessed on: 17 dec. 2023.

DATA SPACES SUPPORT CENTRE (DSSC). **Blueprint Version 0.5**. [S. l.: s. n.], 2023. Available at: <https://dssc.eu/space/BPE/179175433/Data+Spaces+Blueprint+%7C+Version+0.5+%7C+September+2023?attachment=/rest/api/content/179175433/child/attachment/att187400211/download&type=application/pdf&filename=DSSC-Blueprint-Version-1.0.pdf>. Accessed on: 4 nov. 2023.

DATATILSYNET - DANISH DATA PROTECTION AUTHORITY. **Alvorlig kritik af Helsingør Kommune i Chromebook-sag**. [S. l.], 2021. Available at: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/sep/afgoerelse-vedroerende-brudpaa-persondatasikkerheden>. Accessed on: 27 sep. 2023.

DATATILSYNET - DANISH DATA PROTECTION AUTHORITY. **Chromebooks: Datatilsynet suspenderer forbud og giver påbud om lovliggørelse**. [S. l.], 2022a. Available at: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/sep/chromebooks-datatilsynet-suspenderer-forbud-og-giver-paabud-om-lovliggoerelse->. Accessed on: 27 sep. 2023.

DATATILSYNET - DANISH DATA PROTECTION AUTHORITY. **Datatilsynet fastholder forbud i Chromebook-sag**. [S. l.], 2022b. Available at: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/aug/datatilsynet-fastholder-forbud-i-chromebook-sag>. Accessed on: 27 sep. 2023.

DATATILSYNET - DANISH DATA PROTECTION AUTHORITY. **Datatilsynet nedlægger behandlingsforbud i Chromebook-sag**. [S. l.], 2022c. Available at: <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/jul/datatilsynet-nedlaegger-behandlingsforbud-i-chromebook-sag->. Accessed on: 27 sep. 2023.

DATATILSYNET - DANISH DATA PROTECTION AUTHORITY. **Datatilsynet undersøger kommuners materiale om Google Workspace**. [S. l.], 2022d. Available at: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/nov/datatilsynet-undersoeger-kommuners-materiale-om-google-workspace>. Accessed on: 27 sep. 2023.

DATATILSYNET - DANISH DATA PROTECTION AUTHORITY. **Konstruktivt møte om Chromebooks.** [S. l.], 2022e. Available at: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/aug/konstruktivt-moede-om-chromebooks>. Accessed on: 27 sep. 2023.

DATATILSYNET - DANISH DATA PROTECTION AUTHORITY. **Yderligere materiale udsætter afgørelse om Chromebooks.** [S. l.], 2022f. Available at: <https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/dec/yderligere-materiale-udsatter-afgoerelse-om-chromebooks>. Accessed on: 27 sep. 2023.

DATATILSYNET - NORWEGIAN DATA PROTECTION AUTHORITY. **Advance notification of order to rectify unfairly processed and incorrect personal data - International Baccalaureate Organization.** [S. l.: s. n.], 2020a. Available at: <https://www.datatilsynet.no/contentassets/04df776f85f64562945f1d261b4add1b/advance-notification-of-order-to-rectify-unfairly-processed-and-incorrect-personal-data.pdf>. Accessed on: 17 oct. 2023.

DATATILSYNET - NORWEGIAN DATA PROTECTION AUTHORITY. **Bruk av Google Chromebook og G Suite for Education (og andre skytjenester) i grunnskolen.** [S. l.], 2020b. Available at: <https://www.datatilsynet.no/personvern-pa-ulike-omrader/skole-barn-unge/bruk-av-google-chromebook-og-g-suite-for-education-og-andre-skytjenester-i-grunnskolen/>. Accessed on: 5 dec. 2023.

DATATILSYNET - NORWEGIAN DATA PROTECTION AUTHORITY. **Order to provide information – International Baccalaureate Organization – Awarding model and grading system.** [S. l.: s. n.], 2020c. Available at: <https://www.datatilsynet.no/contentassets/ea9284bbfcb64f819b2171228bc912a4/ibo---order-to-provide-information-by-24-july-2020.pdf>. Accessed on: 17 oct. 2023.

DATATILSYNET - NORWEGIAN DATA PROTECTION AUTHORITY. **Varsel om irettesettelse for feil bruk av Googles løsninger i skolen.** [S. l.], 2020d. Available at: <https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/varsel-om-irettesettelse-for-feil-bruk-av-googles-losninger-i-skolen/>. Accessed on: 4 dec. 2023.

DATATILSYNET - NORWEGIAN DATA PROTECTION AUTHORITY. **Varsel om vedtak om irettesettelse - Bruk av G Suite for Education - Sandnes Kommune.** [S. l.: s. n.], 2020e. Available at: <https://www.datatilsynet.no/contentassets/ff4de39da1174e7bb144d7a96027922c/varsel-om-vedtak-om-irettesettelse---bruk-av-g-suite-for-education---sandnes.pdf>. Accessed on: 4 dec. 2023.

DATATILSYNET - NORWEGIAN DATA PROTECTION AUTHORITY. **Varsel om vedtak om irettesettelse - Bruk av Google Chromebook i skolen - Strand Kommune.** [S. l.: s. n.], 2020f. Available at: <https://www.datatilsynet.no/contentassets/ff4de39da1174e7bb144d7a96027922c/varsel-om-vedtak-om-irettesettelse---bruk-av-google-chromebook-i-skolen---strand.pdf>. Accessed on: 4 dec. 2023.

DATATILSYNET - NORWEGIAN DATA PROTECTION AUTHORITY. **Varsel om vedtak om irettesettelse - Bruk av Google Chromebook og G Suite for Education i skolen - Bergen Kommune.** [S. l.: s. n.], 2020g. Available at: <https://www.datatilsynet.no/contentassets/ff4de39da1174e7bb144d7a96027922c/varsel-om-vedtak-om-irettesettelse---bruk-av-google-chromebook-og-g-suite-for-education---bergen2.pdf>. Accessed on: 4 dec. 2023.

DATENSCHUTZKONFERENZ. AG DSK „Microsoft-Onlinedienste“ **Zusammenfassung der Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung.** [S. l.: s. n.], 2022. Available at: https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf. Accessed on: 30 sep. 2023.

DAVENPORT, Thomas H. **Big data @ work: dispelling the myths, uncovering the opportunities.** Boston: Harvard Business Review Press, 2014.

DEDEZADE, E. Microsoft to deliver cloud services from new datacentres in Germany in 2019 to meet evolving customer needs. **Microsoft Stories Europe**, [s. l.], 31 aug. 2018. Available at: <https://news.microsoft.com/europe/2018/08/31/microsoft-to-deliver-cloud-services-from-new-datacentres-in-germany-in-2019-to-meet-evolving-customer-needs/>. Accessed on: 27 sep. 2023.

DENSA, Roberta. Artigo 14. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (org.). **Comentários à Lei Geral de Proteção de Dados Pessoais.** 2. ed. [S. l.]: Editora Foco, 2023. p. 206–224.

DER HESSISCHE BEAUFTRAGTE FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT. **Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Microsoft Office 365 in hessischen Schulen.** [S. l.], 2019a. Available at: <http://web.archive.org/web/20191220095453/https://datenschutz.hessen.de/pressemitteilungen/stellungnahme-des-hessischen-beauftragten-f%C3%BCr-datenschutz-und>. Accessed on: 27 sep. 2023.

DER HESSISCHE BEAUFTRAGTE FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT. **Zweite Stellungnahme zum Einsatz von Microsoft Office 365 in hessischen Schulen.** [S. l.], 2019b. Available at: <http://web.archive.org/web/20221203045150/https://datenschutz.hessen.de/pressemitteilungen/zweite-stellungnahme-zum-einsatz-von-microsoft-office-365-hessischen-schulen>. Accessed on: 27 sep. 2023.

DER LANDESBEAUFTRAGTE FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT BADEN-WÜRTTEMBERG. **Empfehlung des LfDI hinsichtlich der Nutzung der geprüften Version von Microsoft Office 365 an Schulen.** [S. l.], 2021. Available at: <https://www.baden-wuerttemberg.datenschutz.de/lfdi-raet-aufgrund-hoher-datenschutzrechtlicher-risiken-von-der-nutzung-der-geprueften-version-von-microsoft-office-365-an-schulen-ab/>. Accessed on: 27 sep. 2023.

DER LANDESBEAUFTRAGTE FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT BADEN-WÜRTTEMBER. **Hinweise des LfDI zur Nutzung von Microsoft 365 durch Schulen.** [S. l.], 2022. Available at: <https://www.baden-wuerttemberg.datenschutz.de/ms-365-schulen-hinweise-weiteres-vorgehen/>. Accessed on: 27 sep. 2023.

DERECHOS DIGITALES; PRIVACY INTERNATIONAL. **Stakeholder Report -Universal Periodic Review 41st Session-Brazil.** [S. l.: s. n.], 2022. Available at: <https://privacyinternational.org/sites/default/files/2022-11/Final%20Brazil%20UPR.pdf>. Accessed on: 1 nov. 2023.

DIJCK, José van. Datafication, dataism and dataveillance: data between scientific paradigm and ideology. **Surveillance & Society**, [s. l.], v. 12, n. 2, p. 197–208, 2014.

DIJCK, José van. Seeing the forest for the trees: Visualizing platformization and its governance. **New Media and Society**, [s. l.], v. 23, n. 9, p. 2801–2819, 2021.

DIJCK, José van. **The Culture of Connectivity: A Critical History of Social Media.** New York: Oxford University Press, 2013.

DIJCK, José van; POELL, Thomas; WAAL, Martijn de. **The Platform Society.** New York: Oxford University Press, 2018.

DINUM. **Le Cloud pour les administrations.** [S. l.], [s. d.]. Available at: <https://www.numerique.gouv.fr/services/cloud/doctrine/>. Accessed on: 27 sep. 2023.

DISHON, Gideon. New data, old tensions: Big data, personalized learning, and the challenges of progressive education. **Theory and Research in Education**, [s. l.], v. 15, n. 3, p. 272–289, 2017.

D'MELLO, Sidney. Improving student engagement in and with digital learning technologies. *In: OECD DIGITAL EDUCATION OUTLOOK 2021: PUSHING THE FRONTIERS WITH ARTIFICIAL INTELLIGENCE, BLOCKCHAIN AND ROBOTS.* Paris: OECD Publishing, 2021. p. 79–104.

DOEK, Jaap. The CRC General Principles. *In: 18 CANDLES: THE CONVENTION ON THE RIGHTS OF THE CHILD REACHES MAJORITY.* [S. l.]: Institut International des Droits de l'Enfant, 2007. p. 31–38. Available at: <http://www.childsrights.org>.

DPC. **Children front and centre: Fundamentals for a child-oriented approach to data processing.** Dublin: [s. n.], 2021. Available at: https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf. Accessed on: 17 jul. 2023.

DRECHSLER, Laura; ELBI, Abdullah; KINDT, Els; KUN, Eyup; MESZAROS, Janos; VRANCKAERT, Koen. **CiTIP Working Paper Series. Third time is the charm? The draft Data Privacy Framework for international personal data transfers from the European Union to the United States.** KU Leuven Centre for IT & IP Law – imec. 23 may 2023.

Available at: <https://www.law.kuleuven.be/citip/en/docs/books/citip-working-paper-2023-drechsler-elbi-kindt-kun.pdf>. Accessed on: 14 feb. 2024.

DRECHSLER, Laura; VOGIATZOGLU, Plixavra. Quo vadis purpose limitation? *Norra Stockholm Bygg AB v Per Nycander AB*. **European Law Review**, [s. l.], v. 48, n. 4, p. 469–479, 2023.

DUCUING, Charlotte. Beyond the data flow paradigm: governing data requires to look beyond data. **Technology and Regulation**, [s. l.], p. 57–64, 2020. <https://doi.org/10.26116/techreg.2020.006>.

DUCUING, Charlotte; SCHROERS, Jessica. The recent case law of the CJEU on (joint) controllership: have we lost the purpose of “purpose”? **Computerrecht Tijdschrift voor Informatica, Telecommunicatie en Recht**, [s. l.], n. 6, p. 424–429, 2020.

EDPB. **Endorsed WP29 Guidelines**. [S. l.], 2018. Available at: https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en. Accessed on: 27 oct. 2023.

EDPB. **Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. Version 2.0**. [S. l.: s. n.], 2019. Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf. Accessed on: 17 jul. 2023.

EDPB. **Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1**. [S. l.: s. n.], 2020. Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Accessed on: 14 jul. 2023.

EDPB. **Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 2.1**. [S. l.: s. n.], 2021.

EDPB. **Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Version 2.0**. 2021. Available at: https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf. Accessed on: 14 jul. 2023.

ENGLER, Alex. **Enrollment algorithms are contributing to the crises of higher education**. [S. l.: s. n.], 2021. Available at: <https://www.brookings.edu/articles/enrollment-algorithms-are-contributing-to-the-crises-of-higher-education/>. Accessed on: 13 feb. 2024.

ERIKSEN, Thomas Hylland. What’s wrong with the Global South and the Global North? *In*: [S. l.]: Global South Studies Center, University of Cologne, 2015. p. 3–4. Available at: https://kups.ub.uni-koeln.de/6399/1/voices012015_concepts_of_the_global_south.pdf. Accessed on: 20 jun. 2023.

EUROPEAN COMMISSION. **A Europe fit for the digital age: Empowering people with a new generation of technologies**. [S. l.], [s. d.]. Available at:

https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en. Accessed on: 22 oct. 2023 a.

EUROPEAN COMMISSION. **A European approach to artificial intelligence**. [S. l.], 2021a. Available at: <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence#:~:text=The%202021%20review%20of%20the,critical%20component%20of%20AI%20excellence>. Accessed on: 18 dec. 2023.

EUROPEAN COMMISSION. **Antitrust: Commission sends Statement of Objections to Google over abusive practices in online advertising technology**. [S. l.], 2023a. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3207. Accessed on: 14 aug. 2023.

EUROPEAN COMMISSION. **Artificial Intelligence – Questions and Answers**. [S. l.], 2023b. Available at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683. Accessed on: 18 dec. 2023.

EUROPEAN COMMISSION, Directorate-General for Education, Youth, Sport and Culture. **Blended learning for high quality and inclusive primary and secondary education Handbook**. Luxembourg: [s. n.], 2021. Available at: <https://data.europa.eu/doi/10.2766/237842>. Accessed on: 5 nov. 2023.

EUROPEAN COMMISSION. **Commission Staff Working Document Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Digital Education action Plan 2021-2027 Resetting education and training for the digital age. SWD/2020/0209**. [S. l.: s. n.], 2020a. Available at: https://education.ec.europa.eu/sites/default/files/document-library-docs/deap-swd-sept2020_en.pdf#page=3. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. **Commission Staff Working Document on Common European Data Spaces. SWD/2022/45**. Brussels: [s. n.], 2022a. Available at: <https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces>. Accessed on: 4 nov. 2023.

EUROPEAN COMMISSION. **Commission Staff Working Paper. Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and (...)**. Brussels: [s. n.], 2012. Available at: https://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf. Accessed on: 15 jul. 2023.

EUROPEAN COMMISSION. **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A New Skills Agenda for Europe Working together to strengthen human capital, employability and competitiveness. COM/2016/0381**. [S. l.: s.

n.], 2016a. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0381>. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Digital Education Action Plan 2021-2027 Resetting education and training for the digital age. COM/2020/0624.** [*S. l.: s. n.*], 2020b. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0624>. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Fostering a European approach to Artificial Intelligence. COM/2021/205.** [*S. l.*], 2021b. Available at: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2021%3A205%3AFIN>. Accessed on: 18 dec. 2023.

EUROPEAN COMMISSION. **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Improving and Modernising Education. COM/2016/941.** [*S. l.: s. n.*], 2016b. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0941&rid=3>. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Investing in Europe's Youth. COM/2016/940.** [*s. l.*], 2016c. Available at: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52016DC0940>. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a renewed EU agenda for higher education. COM/2017/0247.** [*s. l.*], 2017a. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0247>. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on achieving the European Education Area by 2025. COM/2020/625.** [*S. l.: s. n.*], 2020c. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0625>. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions School development and excellent teaching for a great start in life. COM/2017/0248.** [*s. l.*], 2017b. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A248%3AFIN>. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the**

Committee of the Regions Strengthening European Identity through Education and Culture The European Commission's contribution to the Leaders' meeting in Gothenburg. COM/2017/0673 final. [S. l.: s. n.], 2017c. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A673%3AFIN>. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. **Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Building a stronger Europe: the role of youth, education and culture policies. COM/2018/268.** [S. l.: s. n.], 2018a. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A268%3AFIN>. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. **Coordinated Plan on Artificial Intelligence.** [S. l.], 2021c. Available at: <https://digital-strategy.ec.europa.eu/en/policies/plan-ai>. Accessed on: 18 dec. 2023.

EUROPEAN COMMISSION. **Digital Education Action Plan Factsheet.** [S. l.: s. n.], 2018b. Available at: <https://education.ec.europa.eu/sites/default/files/document-library-docs/digital-education-action-plan-factsheet.pdf>. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. **European Education Area explained.** [S. l.], [s. d.]. Available at: <https://education.ec.europa.eu/about-eea/the-eea-explained>. Accessed on: 22 oct. 2023 b.

EUROPEAN COMMISSION. **European Skills Agenda.** [S. l.], [s. d.]. Available at: <https://ec.europa.eu/social/main.jsp?catId=1223&langId=en>. Accessed on: 22 oct. 2023 c.

EUROPEAN COMMISSION. **Europe's Digital Decade.** [S. l.], [s. d.]. Available at: <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade>. Accessed on: 22 oct. 2023 d.

EUROPEAN COMMISSION. **New measures to boost key competences and digital skills, as well as the European dimension of education.** [S. l.], 2018c. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_102. Accessed on: 22 oct. 2023.

EUROPEAN COMMISSION. **Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive).** [S. l.: s. n.], 2022b. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496>. Accessed on: 18 dec. 2023.

EUROPEAN COMMISSION. **Recovery plan for Europe.** [S. l.], [s. d.]. Available at: https://commission.europa.eu/strategy-and-policy/recovery-plan-europe_en. Accessed on: 22 oct. 2023 e.

EUROPEAN COMMISSION. **White Paper On Artificial Intelligence - A European approach to excellence and trust.** Brussels: [s. n.], 2020d. Available at: https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf. Accessed on: 18 dec. 2023.

EUROPEAN COURT OF HUMAN RIGHTS. **Guide on Article 8 of the European Convention on Human Rights. Right to respect for private and family life, home and correspondence.** [S. l.: s. n.], 2022. Available at: https://www.echr.coe.int/documents/d/echr/Guide_Art_8_ENG. Accessed on: 23 jul. 2023.

EUROPEAN DATA PROTECTION SUPERVISOR (EDPS). **Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the light of legislative developments.** [S. l.: s. n.], 2023. Available at: https://edps.europa.eu/system/files/2023-10/2023-0137_d3269_opinion_en.pdf. Accessed on: 18 dec. 2023.

EUROPEAN PARLIAMENT. **Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI.** [S. l.], 2023. Available at: <https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai>. Accessed on: 18 dec. 2023.

EUROPEAN PARLIAMENT; COUNCIL OF THE EUROPEAN UNION. **Decision (EU) 2023/936 of the European Parliament and of the Council of 10 May 2023 on a European Year of Skills (Text with EEA relevance).** PE/12/2023/REV/1. [S. l.: s. n.], 2023. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023D0936>. Accessed on: 22 oct. 2023.

EUROPEAN UNION. Court of Justice of the European Union. **Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems.** Case C-311/18, ECLI:EU:C:2020:559. 2020. Available at: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3366705>. Accessed on: 14 aug. 2023.

EUROPEAN UNION. Court of Justice of the European Union. **Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV.** Case C-40/17, ECLI:EU:C:2019:629. 2019. Available at: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&doclang=EN>. Accessed on: 14 aug. 2023.

EUROPEAN UNION. Court of Justice of the European Union. **Hans-Dieter Jundt, Hedwig Jundt v. Finanzamt Offenburg.** C-281/06, ECLI:EU:C:2007:816. 2007a. Available at: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=71923&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1226224>. Accessed on: 13 jul. 2023.

EUROPEAN UNION. Court of Justice of the European Union. **Mediakabel BV v. Commissariaat voor de Media.** C-89/04, ECLI:EU:C:2005:348. 2005. Available at: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=60336&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1290702>. Accessed on: 13 jul. 2023.

EUROPEAN UNION. Court of Justice of the European Union. **OQ v Land Hessen.** C-634/21, ECLI:EU:C:2023:957. 2023. Available at: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=280426&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=2565079>. Accessed on: 14 dec. 2023.

EUROPEAN UNION. Court of Justice of the European Union. **Sotiris Papasavvas v. O Fileleftheros Dimosia Etairia Ltd, Takis Kounnafi, Giorgos Sertis**. C-291/13, ECLI:EU:C:2014:2209. 2014. Available at: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=157524&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1225989>. Accessed on: 13 jul. 2023.

EUROPEAN UNION. Court of Justice of the European Union. **Tietosuojavaltuutettu v. Jehovan todistajat — uskonnollinen yhdyskunta**. Case C-25/17, ECLI:EU:C:2018:551. 2018a. Available at: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=203822&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=2929029>. Accessed on: 14 aug. 2023.

EUROPEAN UNION. Court of Justice of the European Union. **Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH**. Case C-210/16, ECLI:EU:C:2018:388. 2018b. Available at: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=2928770>. Accessed on: 14 aug. 2023.

EUROPEAN UNION. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. **Official Journal L 281**: 23 nov. 1995. Available at: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>. Accessed on: 30 dec. 2023.

EUROPEAN UNION. Explanations relating to the Charter of Fundamental Rights. **OJ C 303, 14.12.2007, p. 17–35**: 2007b. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32007X1214%2801%29>. Accessed on: 23 jul. 2023.

EUROPEAN UNION. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. **COM/2021/206**: 2021. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206>. Accessed on: 30 dec. 2023.

EUROPEAN UNION. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)**. European Union: OJ L 119, 4.5.2016, p. 1–88, 4 mai 2016. Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. Accessed on: 19 jul. 2023.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA). **Handbook on European data protection law**. [S. l.: s. n.], 2018. Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf. Accessed on: 18 jul. 2023.

FABBRINI, Federico. The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court. In: VRIES, Sybe de; BERNITZ, Ulf;

WRATHERILL, Stephen (org.). **The EU Charter of Fundamental Rights as a Binding Instrument : Five Years Old and Growing**. Oxford: Hart Publishing, 2015. p. 261–286.

FACEBOOK. **Free Basics**. [S. l.], [s. d.]. Available at: <https://www.facebook.com/connectivity/solutions/free-basics>. Accessed on: 1 aug. 2023.

FADER, Peter; HOYNE, Neil. Important lessons for embracing customer lifetime value. **Think with Google**, [s. l.], aug. 2021. Available at: https://www.thinkwithgoogle.com/marketing-strategies/data-and-measurement/customer-lifetime-value/?utm_source=rss-reader&utm_medium=rss&utm_campaign=rss-feed. Accessed on: 13 aug. 2023.

FEDDERS, Barbara. The Constant and Expanding Classroom: Surveillance in K-12 Public Schools Recommended Citation. **North Carolina Law Review**, [s. l.], v. 97, n. 6, p. 1673–1726, 2019. Available at: <https://scholarship.law.unc.edu/nclr/vol97/iss6/4>. Accessed on: 29 mai 2023.

FEDERAL TRADE COMMISSION (FTC). **FTC Proposes Strengthening Children’s Privacy Rule to Further Limit Companies’ Ability to Monetize Children’s Data**. [S. l.], 2023. Available at: <https://www.ftc.gov/news-events/news/press-releases/2023/12/ftc-proposes-strengthening-childrens-privacy-rule-further-limit-companies-ability-monetize-childrens>. Accessed on: 25 dec. 2023.

FERNANDES, Elora. Crianças e adolescentes na LGPD: Bases legais aplicáveis. **Migalhas**, [s. l.], 27 oct. 2020. Available at: <https://www.migalhas.com.br/depeso/335550/criancas-e-adolescentes-na-lgpd--bases-legais-aplicaveis>. Accessed on: 4 oct. 2023.

FERNANDES, Elora; MEDON, Filipe. Proteção de crianças e adolescentes na LGPD: desafios interpretativos. **Revista Eletrônica da PGE-RJ**, [s. l.], v. 4, n. 2, p. 1–24, 2021.

FERNANDES, Elora; SAS, Martin. **Putting Children First: A Critical Analysis of the European Data Strategy for Educational Data**. Gent: [s. n.], 2023. Available at: <https://lirias.kuleuven.be/handle/20.500.12942/731220>. Accessed on: 14 dec. 2023.

FLORIDI, Luciano. The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. **Philosophy and Technology**, [s. l.], v. 33, n. 3, p. 369–378, 2020.

FLORIDI, Luciano. **The Philosophy of Information**. [S. l.]: Oxford University Press, 2011.

FLYNN, Laurie J. Google to Offer Services for Businesses. **The New York Times**, [s. l.], 28 aug. 2006. Available at: <https://www.nytimes.com/2006/08/28/technology/28google.html>. Accessed on: 8 aug. 2023.

FREEMAN, Michael D. A. Article 3. The Best Interests of the Child. In: ALLEN, André *et al.* (org.). **A Commentary on the United Nations Convention on the Rights of the Child**. Leiden: Martinus Nijhoff, 2007.

FREIRE, Paulo. **Política e educação**. 5. ed. São Paulo: Cortez Editora, 2001. v. 23

GALLAGHER, Sean R *et al.* **Digital Credentials and Talent Acquisition Tech: Closing the Data Gap Between Learning and Hiring**. [S. l.: s. n.], 2023. Available at:

https://cps.northeastern.edu/wp-content/uploads/2023/03/Digital_Credentials_Talent_Acquisition_Tech.pdf. Accessed on: 4 mai 2023.

GASPAR, Walter Britto; MENDONÇA, Yasmin Curzi de. Inteligência Artificial no Brasil ainda precisa de uma estratégia. FGV, Rio de Janeiro, 11 mai 2021. Available at: <https://portal.fgv.br/artigos/inteligencia-artificial-brasil-ainda-precisa-estrategia>. Accessed on: 19 dec. 2023.

GAYK, Betina. **28. Bericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen zum Datenschutz für die Zeit vom 1. Januar 2022 bis zum 31. Dezember 2022 und zur Informationsfreiheit für die Zeit vom 1. Januar 2021 bis zum 31. Dezember 2022.** Düsseldorf : [s. n.], 2023. Available at: https://www.ldi.nrw.de/system/files/media/document/file/28_datenschutzbericht_2023_ldi-nrw_1.pdf. Accessed on: 30 sep. 2023.

GIANNINI, Stefania. **Generative AI and the future of education.** [S. l.: s. n.], 2023. Available at: <https://unesdoc.unesco.org/ark:/48223/pf0000385877>. Accessed on: 27 jul. 2023.

GLEASON, How; HEATH, B K. Injustice embedded in Google Classroom and Google Meet: A techno-ethical audit of remote educational technologies. **Italian Journal of Educational Technology**, [s. l.], v. 29, n. 2, p. 26–41, 2021.

GLOBAL PRIVACY ASSEMBLY (GPA). **43rd Closed Session of the Global Privacy Assembly October 2021. Adopted Resolution on children's digital rights.** [S. l.: s. n.], 2021. Available at: <https://globalprivacyassembly.org/wp-content/uploads/2021/10/20211025-GPA-Resolution-Childrens-Digital-Rights-Final-Adopted.pdf>. Accessed on: 17 dec. 2023.

GOMES, Maria Cecília Oliveira; ZAPPELINI, Thaís Duarte. A LGPD e a obtenção do consentimento dos pais ou responsáveis pela Administração pública em escolas municipais. **Medium CEPI FGV**, [s. l.], 12 sep. 2020. Available at: <https://medium.com/o-centro-de-ensino-e-pesquisa-em-inova%C3%A7%C3%A3o-est%C3%A1-a-lgpd-e-a-obten%C3%A7%C3%A3o-do-consentimento-dos-pais-ou-respons%C3%A1veis-pela-administra%C3%A7%C3%A3o-p%C3%BAblica-em-escolas-b9432ad3ab47>. Accessed on: 4 oct. 2023.

GONZÁLEZ FUSTER, Gloria. Article 18. Right to restriction of processing. In: KUNER, Christopher *et al.* (org.). **The EU General Data Protection Regulation: A Commentary.** [S. l.]: Oxford University Press, 2020. p. 485–491.

GONZÁLEZ FUSTER, Gloria. **The Emergence of Personal Data Protection as a Fundamental Right of the EU.** [S. l.]: Springer, 2014.

GONZÁLEZ FUSTER, Gloria; HIJMANS, Hielke. **The EU rights to privacy and personal data protection: 20 years in 10 questions. Discussion paper.** [S. l.: s. n.], 2019. Available at: https://brusselsprivacyhub.eu/events/20190513.Working_Paper_Gonza%CC%81lez_Fuster_Hijmans.pdf. Accessed on: 23 jul. 2023.

GOOD, Judith. Serving students with special needs better: How digital technology can help. *In: OECD DIGITAL EDUCATION OUTLOOK 2021: PUSHING THE FRONTIERS WITH ARTIFICIAL INTELLIGENCE, BLOCKCHAIN AND ROBOTS*. Paris: OECD Publishing, 2021. p. 123–142. Available at: <https://doi.org/10.1787/589b283f-en>. Accessed on: 13 nov. 2023.

GOOGLE. **Aviso de Privacidade do Google Cloud**. [S. l.], 2023a. Available at: <https://cloud.google.com/terms/cloud-privacy-notice?hl=pt-BR>. Accessed on: 1 oct. 2023.

GOOGLE. **Aviso de Privacidade do Google Workspace for Education**. [S. l.], 2023b. Available at: https://workspace.google.com/intl/pt-br/terms/education_privacy/?hl=pt-BR#privacy-police-revamp-contact. Accessed on: 1 jan. 2024.

GOOGLE. **Choose the right edition for your institution**. [S. l.], 2023a. Available at: <https://edu.google.com/workspace-for-education/editions/compare-editions/>. Accessed on: 10 aug. 2023.

GOOGLE. **Cloud Data Processing Addendum (Customers)**. [S. l.], 2023c. Available at: <https://cloud.google.com/terms/data-processing-addendum>. Accessed on: 1 oct. 2023.

GOOGLE. **Compare Google Workspace editions**. [S. l.], 2023b. Available at: https://support.google.com/a/answer/6043385?hl=en&co=DASHER._Family%3DEducation. Accessed on: 10 aug. 2023.

GOOGLE. **Discover programs dedicated to teacher professional development and student engagement**. [S. l.], 2023c. Available at: https://edu.google.com/intl/ALL_be/for-educators/certification-programs/professional-expertise/?modal_active=none. Accessed on: 10 aug. 2023.

GOOGLE. **DPIA Resource Center - Introduction**. [S. l.], 2023d. Available at: <https://cloud.google.com/privacy/data-protection-impact-assessment>. Accessed on: 27 sep. 2023.

GOOGLE. **Find the best Chromebook for your institution**. [S. l.], 2023e. Available at: https://edu.google.com/intl/ALL_us/chromebooks/find-a-chromebook/. Accessed on: 21 aug. 2023.

GOOGLE. **Get Level 1 Teacher Certification**. [S. l.], 2023f. Available at: https://edu.google.com/for-educators/certification-programs/product-expertise/educator-level1/?modal_active=none. Accessed on: 10 aug. 2023.

GOOGLE. Google Announces Education News at Educause. **News from Google**, [s. l.], 10 oct. 2006a. Available at: http://googlepress.blogspot.com/2006/10/google-announces-education-news-at_10.html. Accessed on: 8 aug. 2023.

GOOGLE. **Google Apps**. [S. l.], 2006b. Available at: <http://web.archive.org/web/20061208110748/https://www.google.com/a/>. Accessed on: 8 aug. 2023.

GOOGLE. Google Introduces New Business Version of Popular Hosted Applications. **News from Google**, [s. l.], 22 feb. 2007. Available at: http://googlepress.blogspot.com/2007/02/google-introduces-new-business-version_22.html. Accessed on: 8 aug. 2023.

GOOGLE. Google Sets Its Sites on Google Apps. **News from Google**, [s. l.], 28 feb. 2008. Available at: http://googlepress.blogspot.com/2008/02/google-sets-its-sites-on-google-apps_28.html. Accessed on: 8 aug. 2023.

GOOGLE. **Google Workspace for Education Core and Additional services**. [S. l.], 2023g. Available at: <https://support.google.com/a/answer/6356441?hl=en>. Accessed on: 13 aug. 2023.

GOOGLE. Introducing Google Workspace and a new set of offerings to better meet your needs. **Google Workspace Updates**, [s. l.], 6 oct. 2020. Available at: <https://workspaceupdates.googleblog.com/2020/10/introducing-google-workspace.html>. Accessed on: 8 aug. 2023.

GOOGLE. **Join a community of passionate teachers to share, find inspiration and learn with them**. [S. l.], 2023h. Available at: https://edu.google.com/for-educators/communities/?modal_active=none. Accessed on: 10 aug. 2023.

GOOGLE. **Make learning more alive with Jamboard**. [S. l.], 2023i. Available at: <https://edu.google.com/jamboard/>. Accessed on: 21 aug. 2023.

GOOGLE. **Our approach to Search**. [S. l.], 2023j. Available at: <https://www.google.com/search/howsearchworks/our-approach/>. Accessed on: 14 aug. 2023.

GOOGLE. **Política de Privacidade**. [S. l.], 2023d. Available at: <https://policies.google.com/privacy?hl=pt-BR>. Accessed on: 1 oct. 2023.

GOOGLE. **Services Summary**. [S. l.], 2023k. Available at: https://workspace.google.com/intl/en/terms/user_features.html. Accessed on: 13 aug. 2023.

GOOGLE. **Termos de Serviço**. [S. l.], 2022. Available at: <https://policies.google.com/terms?hl=pt-BR>. Accessed on: 1 oct. 2023.

GOOGLE. **Termos de Serviço do Google Cloud Platform**. [S. l.], 2023e. Available at: <https://cloud.google.com/terms?hl=pt-br>. Accessed on: 1 oct. 2023.

GOOGLE. **Termos de Serviço do Google Workspace for Education**. [S. l.], 2023f. Available at: https://workspace.google.com/intl/pt-BR/terms/education_terms/. Accessed on: 1 oct. 2023.

GOOGLE. **Transform education with a project you care about as a Certified Innovator**. [S. l.], 2023l. Available at: https://edu.google.com/intl/ALL_be/for-educators/certification-programs/professional-expertise/certified-innovator/?modal_active=none. Accessed on: 10 aug. 2023.

GRABOW, Chip; ROSE, Lisa. The US has had 57 times as many school shootings as the other major industrialized nations combined. **CNN**, [s. l.], 21 mai 2018. Available at:

<https://edition.cnn.com/2018/05/21/us/school-shooting-us-versus-world-trnd/index.html>. Accessed on: 26 dec. 2023.

GRAND VIEW RESEARCH. **Education Technology Market Size, Share & Trends Analysis Report By Sector (Preschool, K-12, Higher Education), By End-user (Business, Consumer), By Type, By Deployment, By Region, And Segment Forecasts, 2023 - 2030**. [S. l.: s. n.], 2023. Available at: <https://www.grandviewresearch.com/industry-analysis/education-technology-market>. Accessed on: 12 nov. 2023.

GROHMANN, Rafael. No MTST, a soberania digital de que fala Morozov. **Outras Palavras**, [s. l.], 1 sep. 2023. Available at: <https://outraspalavras.net/tecnologiaemdisputa/no-mtst-a-soberania-digital-de-que-fala-morozov/>. Accessed on: 23 dec. 2023.

GRONDWETTELIIK HOF. Arrest nr. 26/2023 van 16 februari 2023. Rolnummers : 7494, 7505, 7526 en 7606. 2023. Available at: <https://www.const-court.be/public/n/2023/2023-026n.pdf>. Accessed on: 14 dec. 2023.

HALEY, Keltie. Sharenting and the (Potential) Right to Be Forgotten. **Indiana Law Journal**, [s. l.], v. 95, n. 3, p. 105–1020, 2020. Available at: <https://www.theguardian.com/technology>.

HANSON, Karl; LUNDY, Laura. Does Exactly What it Says on the Tin? A Critical Analysis and Alternative Conceptualisation of the So-called “General Principles” of the Convention on the Rights of the Child. **International Journal of Children’s Rights**, [s. l.], v. 25, n. 2, p. 285–306, 2017.

HARTZOG, Woodrow. **Privacy’s Blueprint: The Battle to Control the Design of New Technologies**. Cambridge: Harvard University Press, 2018-. ISSN 1744-2567.

HARWELL, Drew. Cheating-detection companies made millions during the pandemic. Now students are fighting back. **The Washington Post**, [s. l.], 12 nov. 2020. Available at: <https://www.washingtonpost.com/technology/2020/11/12/test-monitoring-student-revolt/>. Accessed on: 28 mai 2023.

HASKINS, Caroline. Gaggle Knows Everything About Teens And Kids In School. **BuzzFeedNews**, [s. l.], 1 nov. 2019. Available at: <https://www.buzzfeednews.com/article/carolinehaskins1/gaggle-school-surveillance-technology-education>. Accessed on: 23 mai 2023.

HEIDEBRECHT, Sebastian. From Market Liberalism to Public Intervention: Digital Sovereignty and Changing European Union Digital Single Market Governance. **JCMS: Journal of Common Market Studies**, [s. l.], v. 62, n. 1, p. 205–223, 2024. <https://doi.org/10.1111/jcms.13488>.

HEIMANS, Stephen; SINGH, Parlo; KWOK, Henry. Pedagogic rights, public education and democracy. **European Educational Research Journal**, [s. l.], v. 21, n. 1, p. 71–82, 2022.

HELD, William B *et al.* A Material Lens on Coloniality in NLP. *In:* , 2023. **Anais [...]**. [S. l.: s. n.], 2023. Available at: <https://arxiv.org/abs/2311.08391>. Accessed on: 16 nov. 2023.

HENRIQUES, Isabela. **Direitos Fundamentais da Criança no Ambiente Digital: O dever de garantia da absoluta prioridade**. São Paulo: Thompson Reuters Brasil, 2023.

HENRIQUES, Isabella; MEIRA, Marina; HARTUNG, Pedro. A nova LGPD, o seu relevante artigo 14 e as práticas de mercado. *In*: LIMA, Stephane (org.). **Educação, dados e plataformas: análise descritiva dos termos de uso G Suite for Education e Microsoft 365**. São Paulo: Iniciativa Educação Aberta, 2020. p. 11–12. Available at: <https://zenodo.org/records/4012539#.X1EOdpNKi-4>. Accessed on: 3 nov. 2023.

HENRIQUES, Isabella; MEIRA, Marina; HARTUNG, Pedro. A proibição do direcionamento de publicidade microsegmentada para crianças e adolescente e a abusividade do uso de dados pessoais para fins de exploração comercial infanto-juvenil. *In*: LATERÇA, Priscilla *et al.* (org.). **Privacidade e Proteção de Dados de Crianças e Adolescentes**. Rio de Janeiro: Obliq; ITS Rio, 2021. p. 427–453. Available at: <https://itsrio.org/wp-content/uploads/2021/10/Privacidade-e-Protecao-de-Dados-de-Crian%C3%A7as-e-Adolescentes-ITS.pdf>. Accessed on: 3 nov. 2023.

HENRIQUES, Isabella; PITA, Marina; HARTUNG, Pedro. A proteção de dados pessoais de crianças e adolescentes. *In*: MENDES, Laura Schertel *et al.* (org.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Editora Forense, 2020.

HERLO, Bianca; ULLRICH, André; VLADOVA, Gergana. **Sustainable Digital Sovereignty: Interdependencies Between Sustainable Digitalization and Digital Sovereignty**. Berlin: [s. n.], 2023. Available at: Accessed on: 23 dec. 2023.

HEROLD, Benjamin. Google Under Fire for Data-Mining Student Email Messages. **Education Week**, [s. l.], 13 mar. 2014. Available at: <https://www.edweek.org/policy-politics/google-under-fire-for-data-mining-student-email-messages/2014/03>. Accessed on: 10 aug. 2023.

HEROLD, Benjamin. What Is Personalized Learning?. **EducationWeek**, [s. l.], 5 nov. 2019. Available at: <https://www.edweek.org/technology/what-is-personalized-learning/2019/11>. Accessed on: 9 mai 2023.

HESS, Abigail Johnson. Bill and Melinda Gates have spent billions trying to fix U.S. public education but say it's not having the impact they want. **CNCB make it**, [s. l.], 12 feb. 2020. Available at: <https://www.cnn.com/2020/02/12/bill-and-melinda-gates-say-education-philanthropy-is-not-having-impact.html>. Accessed on: 2 jul. 2023.

HESSEL, Stefan. FAQ about telemetry and diagnostic data in Microsoft 365. **Reusch Law**, [s. l.], 17 sep. 2022. Available at: <https://www.reuschlaw.de/en/news/faq-about-telemetry-and-diagnostic-data-in-microsoft-365/>. Accessed on: 27 sep. 2023.

HIGH, Peter. How 174 Year Old Pearson Is Developing The Netflix Of Education. **Forbes**, [s. l.], 20 aug. 2018. Available at: <https://www.forbes.com/sites/peterhigh/2018/08/20/how-174-year-old-pearson-is-developing-the-netflix-of-education/>. Accessed on: 26 dec. 2023.

HILDEBRANDT, Mireille. Defining Profiling: A New Type of Knowledge?. *In*: HILDEBRANDT, M.; GUTWIRTH, S. (org.). **Profiling the European Citizen**. [S. l.]: Springer, 2008. p. 17–45. Available at: www.BioinformaticsWorld.info/feature.

HILDEBRANDT, Mireille. **Smart Technologies and the End(s) of Law**. [S. l.]: Edward Elgar, 2015.

HILLIS, Ken; PETIT, Michael; JARRETT, Kylie. **Google and the Culture of Search**. [S. l.]: Routledge, 2013.

HILLMAN, Velislava. **Edtech procurement matters: It needs a coherent solution, clear governance and market standards**. [S. l.: s. n.], 2022.

HILLMAN, Velislava *et al.* Global transformation, local choices: Navigating the impacts of Artificial Intelligence on education. *In: 2022 ICT IN EDUCATION. SURVEY ON THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES IN BRAZILIAN SCHOOLS*. [S. l.: s. n.], 2023. p. 263–275. Available at: https://cetic.br/media/docs/publicacoes/2/20231122132216/tic_educacao_2022_livro_completo.pdf. Accessed on: 11 dec. 2023.

HLOSTA, Martin *et al.* Predictive learning analytics in online education: A deeper understanding through explaining algorithmic errors. **Computers and Education: Artificial Intelligence**, [s. l.], v. 3, p. 100108, 2022. <https://doi.org/10.1016/j.caeai.2022.100108>.

HOF, Simone Van Der. I Agree... Or Do I? A Rights-Based Analysis of the Law on Children's Consent in the Digital World. **Wisconsin International Law Journal**, [s. l.], v. 32, n. 2, p. 409–445, 2017. Available at: <http://unicef-irc.org/publications/pdf/evolving-eng.pdf>.

HOF, Simone van der; LIEVENS, Eva. The importance of privacy by design and data protection impact assessments in strengthening protection of children's personal data under the GDPR. **Communications Law: The Journal of Computer, Media and Telecommunications Law**, [s. l.], v. 23, n. 1, p. 33–43, 2018. Available at: https://infolawcentre.blogs.sas.ac.uk/files/2018/03/Comms_Law_23.1.pdf. Accessed on: 16 jul. 2023.

HOGAN, Anna; THOMPSON, Greg. Introduction: the “publicness” of schooling. *In: PRIVATISATION AND COMMERCIALISATION IN PUBLIC EDUCATION: HOW THE PUBLIC NATURE OF SCHOOLING IS CHANGING*. [S. l.]: Routledge, 2021.

HOLMES, Wayne *et al.* **Artificial intelligence and education: a critical view through the lens of human rights, democracy and the rule of law**. Strasbourg: [s. n.], 2022. Available at: <https://rm.coe.int/prems-092922-gbr-2517-ai-and-education-txt-16x24-web/1680a956e3>. Accessed on: 9 oct. 2023.

HOLMES, Wayne *et al.* **Technology-enhanced Personalised Learning: Untangling the Evidence**. Stuttgart: [s. n.], 2018. Available at: https://www.bosch-stiftung.de/sites/default/files/publications/pdf/2018-08/Study_Technology-enhanced%20Personalised%20Learning.pdf. Accessed on: 25 dec. 2023.

HOLMES, Wayne. **The Unintended Consequences of Artificial Intelligence**. [S. l.: s. n.], 2023. Available at: <https://www.ei-ie.org/en/item/28115:the-unintended-consequences-of-artificial-intelligence-and-education>. Accessed on: 21 oct. 2023.

HOLMES, Wayne; BIALIK, Maya; FADEL, Charles. **Artificial Intelligence in Education. Promises and Implications for Teaching and Learning**. Boston: [s. n.], 2019. Available at: <https://curriculumredesign.org/our-work/artificial-intelligence-in-education/>. Accessed on: 12 oct. 2023.

HOLONIQ EDUCATION INTELLIGENCE UNIT. **Global EdTech market to reach \$404B by 2025 - 16.3% CAGR**. [S. l.], 2020. Available at: <https://www.holoniq.com/notes/global-education-technology-market-to-reach-404b-by-2025>. Accessed on: 12 nov. 2023.

HOOPER, L.; LIVINGSTONE, S.; POTHONG, K. **Problems with data governance in UK schools: the cases of Google Classroom and ClassDojo**. [S. l.: s. n.], 2022. Available at: <https://digitalfuturescommission.org.uk/wp-content/uploads/2022/08/Problems-with-data-governance-in-UK-schools.pdf>. Accessed on: 27 oct. 2022.

HUMAN RIGHTS WATCH. **“How dare they peep into my private life?”: Children’s Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic**. [S. l.: s. n.], 2022.

ICO. **Age appropriate design: a code of practice for online services**. [S. l.], 2020. Available at: <https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf>. Accessed on: 9 jul. 2023.

ICO. **How to use AI and personal data appropriately and lawfully**. [S. l.], 2022. Available at: <https://ico.org.uk/media/for-organisations/documents/4022261/how-to-use-ai-and-personal-data.pdf>. Accessed on: 19 jul. 2023.

ICO. **The Children’s code and education technologies (edtech)**. [S. l.], 2023a. Available at: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/the-children-s-code-and-education-technologies-edtech/>. Accessed on: 19 jul. 2023.

ICO. **The Children’s code and education technologies (edtech)**. [S. l.], 2023b. Available at: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/the-children-s-code-and-education-technologies-edtech/>. Accessed on: 17 jul. 2023.

IMY. **Beslut efter tillsyn enligt dataskyddsförordningen - Barn- och utbildningsnämnden i Östersunds kommun**. [S. l.: s. n.], 2023a. Available at: <https://www.imy.se/globalassets/dokument/beslut/2023/beslut-om-tillsyn-barn-och-utbildningsforvaltningen-ostersunds-kommun.pdf>. Accessed on: 4 dec. 2023.

IMY. **Sanktionsavgift mot kommun som inte bedömt konsekvenser innan Google Workspace infördes**. [S. l.], 2023b. Available at: <https://www.imy.se/nyheter/sanktionsavgift-mot-kommun-som-inte-bedomt-konsekvenser-innan-google-workspace-infordes/>. Accessed on: 4 dec. 2023.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). **Achieving universal and meaningful digital connectivity. Setting a baseline and targets for 2030**. [S. l.: s. n.], 2022.

Available at: https://www.itu.int/itu-d/meetings/statistics/wp-content/uploads/sites/8/2022/04/UniversalMeaningfulDigitalConnectivityTargets2030_BackgroundPaper.pdf. Accessed on: 11 dec. 2023.

ISAAC, Mike. Facebook Renames Itself Meta. **The New York Times**, [s. l.], 28 oct. 2021. Available at: <https://www.nytimes.com/2021/10/28/technology/facebook-meta-name-change.html>. Accessed on: 18 mar. 2023.

JARKE, Juliane; MACGILCHRIST, Felicitas. Dashboard stories: How narratives told by predictive analytics reconfigure roles, risk and sociality in education. **Big Data and Society**, [s. l.], v. 8, n. 1, 2021.

JOHNSTON, Scott. Introducing Google Drive, the newest member of Google Apps. **Google Cloud Official Blog**, [s. l.], 24 apr. 2012. Available at: <https://cloud.googleblog.com/2012/04/introducing-google-drive-newest-member.html>. Accessed on: 8 aug. 2023.

KEIERLEBER, Mark. Gaggles Surveils Millions of Kids in the Name of Safety. Targeted Families Argue it's 'Not That Smart'. **The 74**, [s. l.], 12 oct. 2021. Available at: <https://www.the74million.org/article/gaggle-surveillance-minneapolis-families-not-smart-ai-monitoring/>. Accessed on 15 jan. 2024.

KERSSENS, Niels K; DIJCK, José van. Governed by Edtech? Valuing Pedagogical Autonomy in a Platform Society. **Harvard Educational Review**, [s. l.], v. 92, n. 2, p. 284–303, 2022.

KIECZA, Daniel. Practice sets: a more personal path to learning. **Google - The Keyword**, [s. l.], 16 mar. 2022. Available at: <https://blog.google/outreach-initiatives/education/introducing-practice-sets/>. Accessed on: 15 jan. 2024.

KIM, Nancy S. **Consentability: Consent and Its Limits**. 1. ed. Cambridge: Cambridge University Press, 2019-. ISSN 1556-5068.

KING, Pippa; PERSON, Jen. **The State of Biometrics 2022: A Review of Policy and Practice in UK Education**. [S. l.: s. n.], 2022. Available at: <https://defenddigitalme.org/wp-content/uploads/2022/05/The-State-of-Biometrics-in-UK-education-2022-v1.7.pdf>. Accessed on: 27 jul. 2023.

KITCHIN, Rob. **The Data Revolution: Big Data, Open Data, Data Infrastructures & their Consequences**. [S. l.]: SAGE Publications, 2014.

KLEEMAN, David. As Kids Kickstart The Metaverse, Is Public Service Media Ready?. **The Children's Media Foundation**, [s. l.], mar. 2021. Available at: <https://www.thechildrensmediafoundation.org/public-service-media-report/articles/as-kids-kickstart-the-metaverse-is-public-service-media-ready>. Accessed on: 18 mar. 2023.

KNOX, Jeremy. Artificial intelligence and education in China. **Learning, Media and Technology**, [s. l.], v. 45, n. 3, p. 298–311, 2020.

KOHL, Uta. The Pixelated Person: Humanity in the Grip of Algorithmic Personalisation. *In: DATA-DRIVEN PERSONALISATION IN MARKETS, POLITICS AND LAW*. [S. l.]: Cambridge University Press, 2021. p. 3–36.

KOHN, Alfie. Four Reasons to Worry About “Personalized Learning”. **Psychology Today**, [s. l.], 24 feb. 2015. Available at: <https://www.psychologytoday.com/intl/blog/the-homework-myth/201502/four-reasons-worry-about-personalized-learning>. Accessed on: 14 mai 2023.

KOMLJENOVIC, Janja *et al.* When public policy ‘fails’ and venture capital ‘saves’ education: Edtech investors as economic and political actors. **Globalisation, Societies and Education**, [s. l.], 2023.

KOSTA, Eleni. Article 8. Conditions applicable to child’s consent in relation to information society services. *In: KUNER, Christopher et al. (org.). The EU General Data Protection Regulation (GDPR): A Commentary*. [S. l.]: Oxford Academic Press, 2020. p. 355–364.

KOTSCHY, Waltraut. Article 6. Lawfulness of processing. *In: KUNER, Christopher et al. (org.). The EU General Data Protection Regulation (GDPR): A Commentary*. [S. l.]: Oxford University Press, 2020. p. 321–344.

KRANENBORG, Herke. Article 8. *In: PEERS, Steve et al. (org.). The EU Charter of Fundamental Rights: A Commentary*. 2. ed. [S. l.]: Hart Publishing, 2021. p. 231–289.

KRUTKA, Daniel G; SMITS, Ryan M; WILLHELM, Troy A. Don’t Be Evil: Should We Use Google in Schools? **TechTrends**, [s. l.], v. 65, p. 421–431, 2021.

KUCIRKOVA, Natalia. OPINION: Some warning flags for those embracing personalized learning powered by education technology. **The Hechinger Report**, [s. l.], 14 oct. 2021. Available at: <https://hechingerreport.org/opinion-some-warning-flags-for-those-embracing-personalized-learning-powered-by-education-technology/>. Accessed on: 16 mar. 2023.

KUCIRKOVA, Natalia. The promise and pitfalls of personalised learning with new EdTech. *In: LIVINGSTONE, Sonia; POTHONG, Kruakae (org.). Education Data Futures: Critical, Regulatory and Practical Reflections*. [S. l.]: Digital Futures Commission, 5Rights Foundation, 2022. p. 221–229. Available at: <https://cms.educationdatafutures.digitalfuturescommission.org.uk/wp-content/uploads/2022/11/Education-Data-Futures.pdf>. Accessed on: 1 aug. 2023.

KUCIRKOVA, Natalia; BROD, Garvin; GAAB, Nadine. Applying the science of learning to EdTech evidence evaluations using the EdTech Evidence Evaluation Routine (EVER). **npj Science of Learning**, [s. l.], v. 8, n. 1, p. 35, 2023. Available at: <https://www.nature.com/articles/s41539-023-00186-7>.

KÜHNE, Thomas. What is a Model?. *In: , 2005, Wadern. Dagstuhl Seminar Proceedings*. Wadern: Schloss Dagstuhl Leibniz Zentrum für Informatik, 2005. p. 1–10. Available at: <https://drops.dagstuhl.de/volltexte/2005/23/pdf/04101.KuehneThomas1.Paper.pdf>. Accessed on: 15 oct. 2023.

LA CHAMBRE DES REPRÉSENTANTS. **Question et réponse écrite n° 55-473: Accord de coopération entre l'APD et la VTC.** [S. l.], 2023. Available at: https://www.stradalex.com/nl/sl_src_publ_div_be_chambre/document/QRcbrb_55-b107-1263-0473-2022202319113. Accessed on: 14 dec. 2023.

LAET, Tinne De. Een kritisch constructief perspectief op Learning Analytics. **Tijdschrift voor Hoger Onderwijs**, [s. l.], v. 41, n. 1, p. 48–60, 2023.

LAET, Tinne De *et al.* Explainable Learning Analytics: challenges and opportunities. *In: , 2020. Companion Proceedings of the 10th International Conference on Learning Analytics & Knowledge LAK20.* [S. l.]: Society for Learning Analytics Research (SoLAR), 2020. p. 500–510. Available at: https://www.solaresearch.org/wp-content/uploads/2020/06/LAK20_Companion_Proceedings.pdf. Accessed on: 3 aug. 2023.

LAET, Tinne de *et al.* “**Learning Analytics**” in het Vlaams Hoger Onderwijs. [S. l.: s. n.], 2018. Available at: https://kvab.be/sites/default/rest/blobs/2122/tw_learninganalytics.pdf. Accessed on: 18 jan. 2023.

LAI, Mei Kuin; SCHILDKAMP, Kim. Data-based Decision: an overview. *In: SCHILDKAMP, Kim; KUIN LAI, Mei; EARL, Lorna (org.). Data-based Decision Making in Education: Challenges and Opportunities.* [S. l.]: Springer, 2013. v. 17, p. 9–21. Available at: <http://www.springer.com/series/6543>.

LAIRD, Elizabeth; DWYER, Madeliene; GRANT-CHAPMAN, Hugh. **Off Task: EdTech Threats to Student Privacy and Equity in the Age of AI.** [S. l.: s. n.], 2023. Available at: <https://cdt.org/insights/report-off-task-edtech-threats-to-student-privacy-and-equity-in-the-age-of-ai/>. Accessed on: 30 nov. 2023.

LAIRD, Elizabeth; QUAY-DE LA VALLEE, Hannah. **Protecting privacy while supporting students who change schools.** [S. l.: s. n.], 2019.

LAMONT, Ruth. Article 24. *In: PEERS, Steve et al. (org.). The EU Charter of Fundamental Rights: A Commentary.* 2. ed. [S. l.]: Hart Publishing, 2021. p. 693–724.

LANGREO, Lauraine. Google Executive: AI Could ‘Transform’ School Into a ‘Personal Learning Experience’. **EducationWeek**, [s. l.], 06 jul. 2023. Available at: <https://www.edweek.org/technology/google-executive-ai-could-transform-school-into-a-personal-learning-experience/2023/07>. Accessed on: 15 jan. 2024.

LANSDOWN, Gerison. **The evolving capacities of the child.** [S. l.]: Save the Children, 2005. Available at: <https://www.unicef-irc.org/publications/384-the-evolving-capacities-of-the-child.html>. Accessed on: 24 jun. 2023.

LAVAL, Christian. **A escola não é uma empresa: o neoliberalismo em ataque ao ensino público.** [S. l.]: Boitempo, 2019.

LAWN, Martin. Voyages of measurement in education in the twentieth century: Experts, tools and centres. **European Educational Research Journal**, [s. l.], v. 12, n. 1, p. 108–119, 2013.

LAWSON, R. Frederic *et al.* **Education**. In: *ENCYCLOPAEDIA BRITANNICA*. [S. l.: s. n.], 2023. Available at: <https://www.britannica.com/topic/education>. Accessed on: 19 mar. 2023.

LAZARE, Melanie. A peek at what's next for Google Classroom. **Google - The Keyword**, [s. l.], 17 feb. 2021a. Available at: <https://blog.google/outreach-initiatives/education/classroom-roadmap/>. Accessed on: 8 aug. 2023.

LAZARE, Melanie. **Learning with Google 2021**. [S. l.], 2021b. Available at: <https://youtu.be/oGEy4PfdZ8?t=2449>. Accessed on: 8 aug. 2023.

LEFÈVRE, Flávia. Soberania e Segurança negligenciadas. **Flávia Lefèvre: Liberdade e direitos na Internet e nas telecomunicações**, [s. l.], 11 mar. 2023. Available at: <https://flavialefevre.com.br/pt/soberania-e-seguranca-negligenciadas>. Accessed on: 23 dec. 2023.

LEI DE DIRETRIZES E BASES DA EDUCAÇÃO NACIONAL. Brazil: 20 dec. 1996. Available at: http://www.planalto.gov.br/ccivil_03/leis/19394.htm. Accessed on: 17 nov. 2023.

LEINONEN, T. **(Critical) history of ICT in education – and where we are heading?**. [S. l.], [s. d.]. Available at: <https://teemuleinonen.fi/2005/06/23/critical-history-of-ict-in-education-and-where-we-are-heading/>. Accessed on: 11 mar. 2023.

LEMAY, David J.; BAEK, Clare; DOLECK, Tenzin. Comparison of learning analytics and educational data mining: A topic modeling approach. **Computers and Education: Artificial Intelligence**, [s. l.], v. 2, 2021.

LEME, Valdir. Cresça com o Google 2019: Transformando o Brasil a partir da capacitação digital. **O Blog do Google Brasil**, [s. l.], 25 feb. 2019. Available at: <https://brasil.googleblog.com/2019/02/cresca-com-o-google-2019.html>. Accessed on: 2 nov. 2023.

LEMOS, Ronaldo *et al.* **Translation of the Brazilian General Data Protection Law**. [S. l.: s. n.], 2020. Available at: https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf. Accessed on: 17 nov. 2023.

LEVIN, Robert A.; HINES, Laurie Moses. Educational Television, Fred Rogers, and the History of Education. **History of Education Quarterly**, [s. l.], v. 43, n. 2, p. 262–275, 2003. Available at: <https://www.jstor.org/stable/3218313>. Accessed on: 16 mai 2023.

LIEVENS, Eva *et al.* Children's Rights and Digital Technologies. In: KILKELLY, Ursula; LIEFAARD, Ton (org.). **International Human Rights of Children**. Singapore: Springer, 2019. p. 487–513.

LIEVENS, Eva. 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**, [s. l.], v. 39, n. 2, p. 128–145, 2021.

LIEVENS, Eva. Wanted: evidence base to underpin a children's rights-based implementation of the GDPR. **Media@LSE**, [s. l.], 14 oct. 2016. Available at:

<https://blogs.lse.ac.uk/medialse/2016/11/10/wanted-evidence-base-to-underpin-a-childrens-rights-based-implementation-of-the-gdpr/>. Accessed on: 14 jul. 2023.

LIEVENS, Eva; VERDOODT, Valerie. Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation. **Computer Law and Security Review**, [s. l.], v. 34, n. 2, p. 269–278, 2018.

LIM, Weng Marc *et al.* Generative AI and the future of education: Ragnarök or reformation? A paradoxical perspective from management educators. **International Journal of Management Education**, [s. l.], v. 21, n. 2, 2023.

LINDH, Maria; NOLIN, Jan. Information We Collect: Surveillance and Privacy in the Implementation of Google Apps for Education. **European Educational Research Journal**, [s. l.], v. 15, n. 6, p. 644–663, 2016.

LIPWORTH, Laurence. **Differences between personalization, customization & individualization**. [S. l.], 2015. Available at: <https://www.linkedin.com/pulse/differences-between-personalization-customization-laurence-lipworth/>. Accessed on: 25 apr. 2023.

LIVINGSTONE, Sonia; LIEVENS, Eva; CARR, John. **Handbook for policy makers on the rights of the child in the digital environment**. [S. l.: s. n.], 2020. Available at: <https://rm.coe.int/publication-it-handbook-for-policy-makers-final-eng/1680a069f8>. Accessed on: 26 jun. 2023.

LIVINGSTONE, Sonia; ÓLAFSSON, Kjartan. **Children's commercial media literacy: new evidence relevant to UK policy decisions regarding the GDPR**. [S. l.: s. n.], 2017. Available at: <https://blogs.lse.ac.uk/medialse/2017/01/26/childrens-commercial-media-literacy-new-evidence-relevant-to-uk-policy-decisions-regarding-the-gdpr/>. Accessed on: 14 jul. 2023.

LIVINGSTONE, Sonia; O'NEILL, Brian. Children's Rights Online: Challenges, Dilemmas and Emerging Directions. In: HOF, Simone van der; BERG, Bibi van den; SCHERMER, Bart (org.). **Minding Minors Wandering the Web: Regulating Online Child Safety**. [S. l.]: Springer, 2014. p. 19–38.

LIVINGSTONE, Sonia; STOILOVA, Mariya. **The 4Cs: Classifying Online Risk to Children**. Hamburg: [s. n.], 2021. Available at: www.ssoar.infoEvidence.https://doi.org/10.21241/ssoar.71817. .

LIVINGSTONE, Sonia; STOILOVA, Mariya; NANDAGIRI, Rishita. **Children's data and privacy online. Growing up in a digital age: An evidence review**. [S. l.: s. n.], 2018. Available at: https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf. Accessed on: 25 jul. 2023.

LOCATELLI, Rita. **Education as a public and common good: reframing the governance of education in a changing context**. [S. l.: s. n.], 2018. Available at: <https://unesdoc.unesco.org/ark:/48223/pf0000261614>. Accessed on: 1 jul. 2023.

LONGPRE, Shayne *et al.* The Data Provenance Initiative: A Large Scale Audit of Dataset Licensing & Attribution in AI. [s. l.], 2023. Available at: <https://arxiv.org/abs/2310.16787v3>. Accessed on: 16 nov. 2023.

LOPES, Gabriel Henrique de Oliveira. **Um olhar sobre as big techs na educação pública: o caso Google for Education na rede de educação básica paulista**. 2023. Dissertação - Universidade Estadual Paulista (UNESP), Marília, 2023. Available at: <https://repositorio.unesp.br/server/api/core/bitstreams/78e16f8c-a2b8-42bb-9c41-149fd96430a6/content>. Accessed on: 16 feb. 2024.

LUBIENSKI, Christopher. What “good” is schooling? The new edu-philanthropies and education reform. In: HOGAN ANNA; THOMPSON, Greg (org.). **Privatisation and Commercialisation in Public Education: How the Public Nature of Schooling in Changing**. [S. l.]: Routledge, 2021.

LUNA, Florencia. Elucidating the Concept of Vulnerability: Layers Not Labels. **International Journal of Feminist Approaches to Bioethics**, [s. l.], v. 2, n. 1, p. 121–139, 2009. Available at: <https://www.jstor.org/stable/40339200>.

LUNDIE, David; ZWITTER, Andrej; GHOSH, Dipayan. Corporatized education and State sovereignty. **Brookings**, [s. l.], 31 jan. 2022. Available at: <https://www.brookings.edu/articles/corporatized-education-and-state-sovereignty/>. Accessed on: 1 jul. 2023.

LUNDY, Laura; BYRNE, Bronagh. The four general principles of the United Nations Convention on the Rights of the Child: the potential value of the approach in other areas of human rights law. In: BREMS, Eva; DESMET ELLEN; VANDENHOLE, Wouter (org.). **Children’s Rights Law in the Global Human Rights Landscape: Isolation, Inspiration, Integration?** [S. l.]: Routledge, 2017. p. 52–70.

LUNDY, Laura; TOBIN, John. Article 29. The Aims of Education. In: TOBIN, John (org.). **The UN Convention on the Rights of the Child**. Oxford: Oxford University Press, 2019.

LUPTON, Deborah; WILLIAMSON, Ben. The datafied child: The dataveillance of children and implications for their rights. **New Media and Society**, [s. l.], v. 19, n. 5, p. 780–794, 2017.

MACENAITE, Milda. From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. **New Media and Society**, [s. l.], v. 19, n. 5, p. 765–779, 2017.

MACENAITE, Milda; KOSTA, Eleni. Consent for processing children’s personal data in the EU: following in US footsteps? **Information and Communications Technology Law**, [s. l.], v. 26, n. 2, p. 146–197, 2017.

MADDOX, Bryan. **The uses of process data in large-scale educational assessments - OECD Education Working Paper No. 286**. [S. l.: s. n.], 2023. Available at: <https://dx.doi.org/10.1787/5d9009ff-en>.

MADIEGA, Tambiama. **Artificial Intelligence Act**. [S. l.: s. n.], 2023. Available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI\(2021\)69879_2_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)69879_2_EN.pdf). Accessed on: 21 oct. 2023.

MAGALHÃES, João Carlos; COULDRY, Nick. Giving by Taking Away: Big Tech, Data Colonialism, and the Reconfiguration of Social Good. **International Journal of Communication**, [s. l.], v. 15, p. 343–362, 2021. Available at: <https://ijoc.org/index.php/ijoc/article/view/15995/3322>. Accessed on: 30 jun. 2023.

MAGID, Larry. Google Classroom Offers Assignment Center for Students and Teachers. **Forbes**, [s. l.], 6 mai 2014. Available at: <https://www.forbes.com/sites/larrymagid/2014/05/06/google-classroom-offers-control-center-for-students-and-teachers/>. Accessed on: 8 aug. 2023.

MALGIERI, Gianclaudio; NIKLAS, Jędrzej. Vulnerable data subjects. **Computer Law and Security Review**, [s. l.], v. 37, 2020.

MARRAFON, Marco Aurélio; FERNANDES, Elora Raad. A, B, C, Google: Riscos ao Direito Fundamental à Proteção de Dados de Crianças e Adolescentes no G Suite for Education. **Revista Direito Público**, [s. l.], v. 17, n. 95, p. 202–229, 2020.

MARSH, Julie A; PANE, John F; HAMILTON, Laura S. **Making Sense of Data-Driven Decision Making in Education: Evidence from Recent RAND Research**. [S. l.: s. n.], 2006. Available at: https://www.rand.org/pubs/occasional_papers/OP170.html. Accessed on: 18 mai 2023.

MASCHERONI, Giovanna. Datafied childhoods: Contextualising datafication in everyday life. **Current Sociology**, [s. l.], v. 68, n. 6, p. 798–813, 2020. <https://doi.org/10.1177/0011392118807534>

MASSÉ, Estelle. **Four Years Under the EU GDPR: How to Fix its Enforcement**. [S. l.: s. n.], 2022. Available at: <https://www.accessnow.org/wp-content/uploads/2022/07/GDPR-4-year-report-2022.pdf>. Accessed on: 29 sep. 2023.

MATSUMI, Hideyuki; SOLOVE, Daniel J. **The Prediction Society: AI and the Problems of Forecasting the Future**. [S. l.: s. n.], 2024. <http://dx.doi.org/10.2139/ssrn.4453869>.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data: A Revolution that will transform how we live, work and think**. E-booked. [S. l.]: Houghton Mifflin Harcourt Publishing, 2013.

MAZZUCATO, Mariana. **Governing Missions in the European Union**. [S. l.: s. n.], 2019. Available at: https://www.kowi.de/de/Portaldata/2/Resources/Horizon2020/mazzucato_report_2019.pdf. Accessed on: 27 sep. 2023.

MAZZUCATO, Mariana. **Mission Economy: A Moonshot Guide to Changing Capitalism**. [S. l.]: Allen Lane, an imprint of Penguin Books, 2021.

MAZZUCATO, Mariana. **Mission-oriented public procurement: international examples**. [S. l.: s. n.], 2020. Available at: https://www.ucl.ac.uk/bartlett/public-purpose/sites/public-purpose/files/final_mission-oriented_public_procurement_international_examples.pdf.

Accessed on: 27 sep. 2023.

MAZZUCATO, Mariana; COLLINGTON, Rosie. **The Big Con: How the Consulting Industry Weakens Our Businesses, Infantilizes Our Governments, and Warps Our Economies**. New York: Penguin Press, 2023.

MCGREGOR, Sean. **Incident 43: Racist AI behaviour is not a new problem**. [S. l.], [s. d.]. Available at: <https://incidentdatabase.ai/cite/43/>. Accessed on: 18 oct. 2023.

MCMULLAN, Scott. More great apps for Google Apps. **Google Cloud Official Blog**, [s. l.], 9 mar. 2010. Available at: <https://cloud.googleblog.com/2010/03/more-great-apps-for-google-apps.html>. Accessed on: 8 aug. 2023.

MEANS, Alexander J. Platform learning and on-demand labor: sociotechnical projections on the future of education and work. **Learning, Media and Technology**, [s. l.], v. 43, n. 3, p. 326–338, 2018.

MEC. **Define critérios e procedimentos para a produção, recepção, avaliação e distribuição de recursos educacionais abertos ou gratuitos voltados para a educação básica em programas e plataformas oficiais do Ministério da Educação**. 16 mai 2018. Available at: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/14729210/do1-2018-05-17-portaria-n-451-de-16-de-maio-de-2018-14729206. Accessed on: 17 nov. 2023.

MEJIAS, Ulises A.; COULDRY, Nick. Datafication. **Internet Policy Review**, [s. l.], v. 8, n. 4, 2019.

MENDONÇA, Júlia; RIELLI, Mariana. A LGPD no Congresso após 4 anos de promulgação e 2 anos de vigência. **Jota**, [s. l.], 7 sep. 2022. Available at: <https://www.jota.info/opiniao-e-analise/artigos/a-lgpd-no-congresso-apos-4-anos-de-promulgacao-e-2-anos-de-vigencia-07092022>. Accessed on: 5 oct. 2023.

MENEZES, Joyceane Bezerra de; RODRIGUES, Francisco Luciano Lima; BODIN DE MORAES, Maria Celina. A capacidade civil e o sistema de apoios no Brasil. **civilistica.com**, [s. l.], v. 10, n. 1, 2021. Available at: <https://civilistica.emnuvens.com.br/redc/article/view/705>. Accessed on: 4 oct. 2023.

MEYER, Marisa *et al.* How educational are “educational” apps for young children? App store content analysis using the Four Pillars of Learning framework. **Journal of Children and Media**, [s. l.], v. 15, n. 4, p. 526–548, 2021.

MEYER, Anneke. The moral rhetoric of childhood. **Childhood**, [s. l.], v. 14, n. 1, p. 85–104, 2007.

MIAO, Fengchun *et al.* **AI and education: guidance for policy-makers**. [S. l.]: UNESCO, 2021. Available at: <https://unesdoc.unesco.org/ark:/48223/pf0000376709>. Accessed on: 29 jul. 2023.

MILAN, Stefania; TRERÉ, Emiliano. Big Data from the South(s): Beyond Data Universalism. **Television and New Media**, [s. l.], v. 20, n. 4, p. 319–335, 2019.

MILKAITE, Ingrida. **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**. 2021. - Ghent University. Faculty of Law and Criminology, Ghent, 2021. Available at: <http://hdl.handle.net/1854/LU-8714018>. Accessed on: 26 jun. 2023.

MILKAITE, Ingrida; LIEVENS, Eva. Child-friendly transparency of data processing in the EU: from legal requirements to platform policies. **Journal of Children and Media**, [s. l.], v. 14, n. 1, p. 5–21, 2020.

MINISTERIE VAN ONDERWIJS, Cultuur en Wetenschap. **Stand van zaken DPIA Google Workspace for Education**. [S. l.: s. n.], 2023. Available at: <https://www.rijksoverheid.nl/documenten/kamerstukken/2023/04/20/stand-van-zaken-dpia-google-workspace-for-education>. Accessed on: 27 sep. 2023.

MINISTÉRIO DA CIÊNCIA, Tecnologia, Inovações e Comunicações. **Estratégia Brasileira para a Transformação Digital. E-Digital**. Brazil: 2018. Available at: <https://www.gov.br/mcti/pt-br/centrais-de-conteudo/comunicados-mcti/estrategia-digital-brasileira/estrategiadigital.pdf>. Accessed on: 17 nov. 2023.

MINISTÉRIO DA TRANSPARÊNCIA, Fiscalização e Controladoria-Geral da União. **3o Plano de Ação Nacional**. [S. l.: s. n.], 2016. Available at: https://www.gov.br/cgu/pt-br/governo-aberto/noticias/2017/3o-plano-de-acao-nacional-na-parceria-para-governo-aberto/plano_port_web-3.pdf/@@download/file/plano_port_web-3.pdf. Accessed on: 17 nov. 2023.

MINISTRY OF EDUCATION, Culture and Science. **Re: Advice from the Dutch Data Protection Authority on Google G Suite for Education**. [S. l.: s. n.], 2021. Available at: https://dataethics.eu/wp-content/uploads/2021/06/Advies_Autoriteit_Persoonsgegevens_inzake_Google_G_Suite_for_Education_EN-1.pdf. Accessed on: 27 sep. 2023.

MITCHELL, Clark. Students of color are getting flagged to their teachers because testing software can't see them. **The Verge**, [s. l.], 9 apr. 2021. Available at: <https://www.theverge.com/2021/4/8/22374386/proctorio-racial-bias-issues-opencv-facial-detection-schools-tests-remote-learning>. Accessed on: 18 oct. 2023.

MITTELSTADT, Brent Daniel. From Individual to Group Privacy in Big Data Analytics. **Philosophy & technology**, Dordrecht, v. 30, n. 4, p. 475–494, 2017. <https://doi.org/10.1007/s13347-017-0253-7>.

MITTELSTADT, Brent Daniel; ALLO, Patrick; TADDEO, Mariarosaria; WACHTER, Sandra; FLORIDI, Luciano. The ethics of algorithms: Mapping the debate. **Big Data & Society**, v. 3, n. 2, p. 1-21, 2016. <https://doi.org/10.1177/2053951716679679>.

MOHAMED, Shakir; PNG, Marie Therese; ISAAC, William. Decolonial AI: Decolonial Theory as Sociotechnical Foresight in Artificial Intelligence. **Philosophy and Technology**, [s. l.], n. 405, p. 1–28, 2020.

MOLENAAR, Inge. Personalisation of learning: Towards hybrid human-AI learning technologies. In: OECD DIGITAL EDUCATION OUTLOOK 2021 PUSHING THE FRONTIERS WITH ARTIFICIAL INTELLIGENCE, BLOCKCHAIN AND ROBOTS. [S. l.]: OECD, 2021. p. 57–77.

MONDRAGON RUIZ, Sofia. **The Effects of Childhood Nostalgia on Brand Loyalty**. 2021. - University of Kent, [s. l.], 2021.

MOSCO, Vincent. **Becoming Digital: Toward a Post-Internet Society**. [S. l.]: Emerald Publishing, 2017.

MOWBRAY, Jacqueline. Is there a right to public education?. In: ADAMSON, Frank *et al.* (org.). **Realizing the Abidjan Principles on the Right to Education**. [S. l.]: Edward Elgar Publishing, 2021.

MRTEE. Beschluss des OVG NRW zum Google Workspace for Education Fall veröffentlicht. **Datenschutz – Schule – News**, [s. l.], 26 jul. 2023a. Available at: <https://news.datenschutz-schule.info/2023/07/26/beschluss-des-ovg-nrw-zum-google-workspace-for-education-fall-veroeffentlicht/>. Accessed on: 27 sep. 2023.

MRTEE. **Dortmunder Gymnasium erhält Weisung der Bezirksregierung, die Nutzung von Google Workspace for Education einzustellen**. [S. l.], 2023b. Available at: <https://news.datenschutz-schule.info/2023/03/24/dortmunder-gymnasium-erhaelt-weisung-der-bezirksregierung-die-nutzung-von-google-workspace-for-education-einzustellen/>. Accessed on: 27 sep. 2023.

MUKHERJEE, S.,; POTHONG, K.,; LIVINGSTONE, S. **Child Rights Impact Assessment: A tool to realise children’s rights in the digital environment**. London: [s. n.], 2021.

MUMFORD, Densua. Data colonialism: compelling and useful, but whither epistemes? **Information Communication and Society**, [s. l.], v. 25, n. 10, p. 1511–1516, 2022.

MURAILLE, Marcel. **From emergency remote learning to a new digital education action plan: an EU attempt to mainstream equality into education**. [S. l.: s. n.], 2020. Available at: <https://www.egmontinstitute.be/from-emergency-remote-learning-to-a-new-digital-education-action-plan/>. Accessed on: 4 nov. 2023.

NAS, Sjoera. Google mitigates 8 high privacy risks for Workspace for Education. [s. l.], 9 aug. 2021. Available at: <https://www.privacycompany.eu/blogpost-en/google-mitigates-8-high-privacy-risks-for-workspace-for-education>. Accessed on: 27 sep. 2023.

NAS, Sjoera; TERRA, Floor. **DPIA on the use of Google G Suite (Enterprise) for Education. For the University of Groningen and the Amsterdam University of Applied Sciences.** [S. l.: s. n.], 2021. Available at: <https://www.surf.nl/files/2021-06/updated-g-suite-for-education-dpia-12-march-2021.pdf>. Accessed on: 27 sep. 2023.

NAS, Sjoera; TERRA, Floor. **Update DPIA report Google Workspace for Education 2 August 2021.** [S. l.: s. n.], 2021. Available at: <https://www.surf.nl/files/2021-08/update-dpia-report-2-august-2021.pdf>. Accessed on: 27 sep. 2023.

NAS, Sjoera; TERRA, Floor. **Verification report Google remediation measures Workspace for Education. For SURF and SIVON.** [S. l.: s. n.], 2023. Available at: <https://sivon.nl/wp-content/uploads/2023/07/20230724-clean-Workspace-for-Education.pdf>. Accessed on: 27 sep. 2023.

NASCIMENTO, Houldine. Governo faz parceria com Google para ferramentas educacionais. **Poder 360**, [s. l.], 20 jun. 2022. Available at: <https://www.poder360.com.br/governo/governo-faz-parceria-com-google-para-ferramentas-educacionais>. Acesso em 11 dec. 2023.

NATIONS UNIES. **Chapitre IV Droits de L’homme. 11. Convention relative aux droits de l’enfant. New York, 20 novembre 1989.** [S. l.], 2023. Available at: https://treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-11&chapter=4. Accessed on: 5 jul. 2023.

NEGRI, Sérgio Marcos Carvalho de Ávila. Robot as Legal Person: Electronic Personhood in Robotics and Artificial Intelligence. **Frontiers**, [s. l.], v. 8, p. 1–10, 2021.

NEGRI, Sergio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. Decisões automatizadas e a proteção de crianças e adolescentes. *In*: LATERÇA, Priscilla *et al.* (org.). **Privacidade e Proteção de Dados de Crianças e Adolescentes.** [S. l.]: Obliq; ITS Rio, 2021.p. 107–137. Available at: <https://itsrio.org/wp-content/uploads/2021/10/Privacidade-e-Protecao-de-Dados-de-Crian%C3%A7as-e-Adolescentes-ITS.pdf>. Accessed on: 28 oct. 2023.

NEGRI, Sergio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon; FERNANDES, Elora. Portabilidade e proteção de dados pessoais: tensões entre pessoa e mercado. **civilistica.com**, [s. l.], v. 10, n. 1, p. 1–39, 2021. Available at: <https://civilistica.emnuvens.com.br/redc/article/view/532/527>. Accessed on: 28 oct. 2023.

NICHOLS, T Philip; GARCIA, Antero. Platform Studies in Education. **Harvard Educational Review**, [s. l.], v. 92, n. 2, p. 209–230, 2022. Available at: <http://meridian.allenpress.com/her/article-pdf/92/2/209/3117145/i1943-5045-92-2-209.pdf>.

NIEMCZYK, Jerzy; TRZASKA, Rafał. Klasyfikacja modeli biznesowych w Industry 4.0 [Business models classification in Industry 4.0]. *In*: URBANEK, Grzegorz; GREGORCZYK, Sylwester (org.). **Zarządzanie strategiczne w dobie cyfrowej gospodarki sieciowej [Strategic management in the digital age of the networked economy].** [S. l.]: Wydawnictwo Uniwersytetu Łódzkiego, 2020.

NIESTADT, Maria. **The new European strategy for a better internet for kids (BIK+)**. [S. l.: s. n.], 2022. Available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733663/EPRS_BRI\(2022\)733663_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733663/EPRS_BRI(2022)733663_EN.pdf). Accessed on: 4 nov. 2023.

NOLAN, Jason; RAYNES-GOLDIE, Kate; MCBRIDE, Melanie. The Stranger Danger: Exploring Surveillance, Autonomy, and Privacy in Children's Use of Social Media. **Journal of Childhood Studies**, [s. l.], v. 36, n. 2, p. 24–32, 2011.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. **Educação em um cenário de plataformização e de economia de dados: parcerias e assimetrias**. São Paulo: [s. n.], 2022. Available at: https://cgi.br/media/docs/publicacoes/1/20221129114057/educacao_em_um_cenario_de_plataformiza%C3%A7ao_e_de_economia_de_dados_parcerias_e_assimetrias.pdf. Accessed on: 31 oct. 2023.

NÚCLEO DE TECNOLOGIA DO MTST. **Homeless Worker Movement in Brazil and the struggle for digital sovereignty**. [S. l.: s. n.], 2023. Available at: <https://nucleodetecnologia.com.br/docs/Cartilha-MTSTec-ENG.pdf>. Accessed on: 23 dec. 2023.

NYST, Carly; GOROSTIAGA, Amaya; GEARY, Patrick. **Industrial Toolkit. Children's Online Privacy and Freedom of Expression**. [S. l.: s. n.], 2018. Available at: [https://sites.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression\(1\).pdf](https://sites.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf). Accessed on: 3 aug. 2023.

OBSERVATÓRIO EDUCAÇÃO VIGIADA. **Abocet**. [S. l.], [s. d.]. Available at: <https://educacaovigiada.org.br/en/abocet.html>. Accessed on: 1 nov. 2023.

OECD. **OECD Digital Education Outlook 2021. Pushing the frontiers with AI, blockchain, and robots**. Paris: OECD Publishing, 2021. (OECD Digital Education Outlook). Available at: https://www.oecd-ilibrary.org/education/oecd-digital-education-outlook-2021_589b283f-en. Accessed on: 30 jul. 2023.

O'NEIL, Cathy. **Weapons of math destruction: how big data increases inequality and threatens democracy**. New York: Crown Publishers, 2016.

O'REILLY, Tim; STRAUSS, Ilan; MAZZUCATO, Mariana. **Algorithmic Attention Rents: A theory of digital platform market power**. [S. l.: s. n.], 2023. Available at: <https://www.ucl.ac.uk/bartlett/public-purpose/wp2023-10>. .

PALMER, Jason. Why I'm Still Bullish About the State of Edtech. **EdSurge**, [s. l.], 1 apr. 2022. Available at: <https://www.edsurge.com/news/2022-04-01-why-i-m-still-bullish-about-the-state-of-edtech>. Accessed on: 20 dec. 2023.

PANE, John F. **Strategies for Implementing Personalized Learning While Evidence and Resources Are Underdeveloped**. [S. l.: s. n.], 2018. Available at: <https://www.rand.org/pubs/perspectives/PE314.html>. Accessed on: 7 jun. 2023.

PANGARKAR, Tajammul. Eye-Opening EdTech Statistics: Opportunities and Obstacles. **Market.US**, [s. l.], 9 mai 2023. Available at: <https://scoop.market.us/edtech-statistics/>. Accessed on: 12 nov. 2023.

PANGRAZIO, Luci *et al.* Datafication Meets Platformization: Materializing Data Processes in Teaching and Learning. **Harvard Educational Review**, [s. l.], v. 92, n. 2, 2022. Available at: <http://meridian.allenpress.com/her/article-pdf/92/2/257/3117141/i1943-5045-92-2-257.pdf>.

PANGRAZIO, Luci; SELWYIN, Neil; CUMBO, Bronwyn. A patchwork of platforms: mapping data infrastructures in schools. **Learning, Media and Technology**, [s. l.], 2022.

PAPAMITSIOU, Zacharoula; ECONOMIDES, Anastasios A. Learning Analytics and Educational Data Mining in Practice: A Systematic Literature Review of Empirical Evidence. **Educational Technology & Society**, [s. l.], v. 17, n. 4, p. 49–64, 2014.

PAPPANO, Laura. The year of the MOOC. **The New York Times**, [s. l.], 2 nov. 2012. Available at: <https://www.nytimes.com/2012/11/04/education/edlife/massive-open-online-courses-are-multiplying-at-a-rapid-pace.html>. Accessed on: 18 mar. 2023.

PATIL, Lara. The business of development: The institutional rationales of technology corporations in educational development. **International Journal of Educational Development**, [s. l.], v. 97, 2023.

PAYNE, Lisa. Child rights impact assessment as a policy improvement tool. **International Journal of Human Rights**, [s. l.], v. 23, n. 3, p. 408–424, 2019.

PECKHAM, Erik. A multiverse, not the metaverse. **Techcrunch**, [s. l.], 25 feb. 2020. Available at: https://techcrunch.com/2020/02/25/virtual-worlds-intro/?guce_referrer=aHR0cHM6Ly93d3cudGhlY2hpbGRyZW5zbWVkaWFmb3VuZGF0aW9uLm9yZy8&guce_referrer_sig=AQAAAIID7jbCgK35d7vQt6HGpaPMn-1KzyoGS4qPB62SemPoCJHxG6siT4ZxXE05gzJx3SsuA1wyNEuPxx56g87VYqQw3TnpYZvIMRCuwUbTA3EymQRIRpCBz_BDkTB6ZE2je3eAHWgZuwoPbEgSbGd32CtIsyeQgGVmFyij9C3s-XveE&guccounter=2. Accessed on: 18 mar. 2023.

PEDRÓ, Francesc *et al.* **Working Papers on Education Policy. Artificial Intelligence in Education: Challenges and Opportunities for Sustainable Development**. Paris: [s. n.], 2019. Available at: <https://unesdoc.unesco.org/ark:/48223/pf0000366994>. Accessed on: 17 dec. 2023.

PEREIRA, Fábio Queiroz; LARA, Mariana Alves; RODRIGUES, Anna Luísa Braz. A autonomia progressiva de crianças e adolescentes e a busca por um sistema de apoios. **civilistica.com**, [s. l.], v. 12, n. 2, p. 1–23, 2023. Available at: <https://civilistica.emnuvens.com.br/redc/article/view/889>. Accessed on: 4 oct. 2023.

PERERA, Ayesh. **The Pygmalion Effect: Definition & Examples**. [S. l.], 2023. Available at: <https://simplysociology.com/pygmalion-effect.html>. Accessed on: 19 mai 2023.

PEREZ, Sarah. Google Expands Its Educational Platform “Classroom” With A New API, Share Button For Websites. **Tech Crunch**, [s. l.], 29 jun. 2015. Available at:

<https://techcrunch.com/2015/06/29/google-expands-its-educational-platform-classroom-with-a-new-api-share-button-for-websites/>. Accessed on: 8 aug. 2023.

PEREZ, Sarah; LARDINOIS, Frederic. Google rebrands its business apps as G Suite, upgrades apps & announces Team Drive. **Tech Crunch**, [s. l.], 29 sep. 2016. Available at: <https://techcrunch.com/2016/09/29/google-rebrands-its-business-apps-as-g-suite-launches-team-drive-upgrades-apps/>. Accessed on: 8 aug. 2023.

PERROTTA, Carlo *et al.* Automation, APIs and the distributed labour of platform pedagogies in Google Classroom. **Critical Studies in Education**, [s. l.], v. 62, n. 1, p. 97–113, 2021.

PERROTTA, C.; EVANS, M. A. Orchestration, power, and educational technology: A response to Dillenbourg. **Computers and Education**, [s. l.], v. 69, p. 520–522, 2013.

PERROTTA, Carlo; WILLIAMSON, Ben. The social life of Learning Analytics: cluster analysis and the ‘performance’ of algorithmic education. **Learning, Media and Technology**, [s. l.], v. 43, n. 1, p. 3–16, 2018.

PETERS, Michael A. The New Prudentialism in Education: Actuarial Rationality and the Entrepreneurial Self. **Educational Theory**, [s. l.], v. 55, n. 2, p. 123–137, 2005.

PINTO, Renata Ávila. Digital Sovereignty or Digital Colonialism?. **Sur**, [s. l.], v. 15, n. 27, p. 15–27, 2018. Available at: <https://sur.conectas.org/soberania-digital-ou-colonialismo-digital/>. Accessed on: 14 sep. 2023.

POORTVLIET, Jos. Microsoft and Telekom no longer offer cloud storage under German jurisdiction. **Nextcloud**, [s. l.], 4 sep. 2018. Available at: <https://nextcloud.com/blog/microsoft-and-telekom-no-longer-offer-cloud-storage-under-german-jurisdiction/>. Accessed on: 27 sep. 2023.

POWLES, Julia; NISSENBAUM, Helen. The Seductive Diversion of ‘Solving’ Bias in Artificial Intelligence. **OneZero Medium**, [s. l.], 7 dec. 2018. Available at: <https://onezero.medium.com/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53>. Accessed on: 18 jan. 2024.

PROJECT GUTENBERG. **Aboc.** [S. l.], [s. d.]. Available at: <https://www.gutenberg.org/about/>. Accessed on: 11 mar. 2023.

PURTOVA, Nadya; MAANEN, Gijss van. Data as an economic good, data as a commons, and data governance. **Law, Innovation, and Technology (Advance online publication)**, [s. l.], v. 16, n. 1, 2023.

QINGDAO DECLARATION, 2015: SEIZE DIGITAL OPPORTUNITIES, LEAD EDUCATION TRANSFORMATION. . [S. l.: s. n.], 2015. Available at: <https://unesdoc.unesco.org/ark:/48223/pf0000233352>. Accessed on: 17 dec. 2023.

REQUIÃO, Maurício; MENDONÇA, Júlia. O caminho mais adequado para o tratamento de dados pessoais de crianças e adolescentes: aplicação do artigo 11 da LGPD e a equiparação com dados sensíveis. **Diké**, [s. l.], v. 22, n. 22, p. 291–304, 2023. Available at: <https://www.dataprivacybr.org/wp->

RICAURTE, Paola. Data Epistemologies, The Coloniality of Power, and Resistance. **Television and New Media**, [s. l.], v. 20, n. 4, p. 350–365, 2019.

RIEDER, Gernot; SIMON, Judith. Big Data: A New Empiricism and its Epistemic and Socio-Political Consequences. *In*: BERECHENBARKEIT DER WELT? [S. l.]: Springer Fachmedien Wiesbaden, 2017. p. 85–105.

RIVAS, Axel. **In-Progress Reflection No. 46 On Current and Critical Issues in Curriculum, Learning and Assessment. The Platformization of Education: A framework to Map the New Directions of Hybrid Education Systems. IBE/2021/WP/CD/46 Learning and Assessment.** [S. l.: s. n.], 2021. Available at: <https://unesdoc.unesco.org/ark:/48223/pf0000377733>. Accessed on: 11 dec. 2023.

ROONEY, Tanya. Trusting children: How do surveillance technologies alter a child's experience of trust, risk and responsibility. **Surveillance & Society**, [s. l.], v. 7, n. 3/4, p. 344–355, 2010.

SAETTLER, L. Paul. **The evolution of American educational technology.** 2. ed. [S. l.]: Information Age Publishing, 2004.

SAHA, Debanjan. How The World Became Data-Driven, And What's Next. **Forbes**, [s. l.], 20 mai 2020. Available at: <https://www.forbes.com/sites/googlecloud/2020/05/20/how-the-world-became-data-driven-and-whats-next/>. Accessed on: 21 jul. 2023.

SALOMON, Jean Jacques. What is technology? The issue of its origins and definitions. **History and Technology**, [s. l.], v. 1, n. 2, p. 113–156, 1984.

SANDBERG, Kirsten. The convention on the rights of the child and the vulnerability of children. **Nordic Journal of International Law**, [s. l.], v. 84, n. 2, p. 221–247, 2015.

SARTOR, Giovanni. **The impact of the General Data Protection Regulation (GDPR) on artificial intelligence.** Brussels: [s. n.], 2020. Available at: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf). Accessed on: 18 jan. 2024.

SARWAR, Moizza Binat. Reading Audrey Watters: A reflection on personalised learning via education technology through a decolonial lens. [s. l.], 21 apr. 2022. Available at: <https://edtechhub.org/2022/04/21/personalised-learning/>. Accessed on: 14 mai 2023.

SAVILLO, Lia. A Chinese School Made Students Wear Brainwave-Detecting Headgear. **Vice**, [s. l.], 4 nov. 2019. Available at: <https://www.vice.com/en/article/a359w4/chinese-school-made-students-wear-brainwave-detecting-headgear>. Accessed on 15 jan. 2014.

SCHAEFER, Joe. A Data-Driven Approach Could Be the Next Great Innovation for Education. **Wired**, [s. l.], [s. d.]. Available at: <https://www.wired.com/sponsored/story/a-data-driven-approach-could-be-the-next-great-innovation-for-education/>. Accessed on: 5 mai 2023.

SCHILDKAMP, Kim; KUIN LAI, Mei. Introduction. *In*: SCHILDKAMP, Kim; KUIN LAI, Mei; EARL, Lorna (org.). **Data-based Decision Making in Education: Challenges and Opportunities.** [S. l.]: Springer, 2013. v. 17, p. 1–8.

SCHMAHL, Stefanie. **United Nations Convention on the Rights of the Child: Article-by-Article Commentary**. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG, 2021.

SCHNEIER, Bruce. Surveillance Kills Freedom By Killing Experimentation. **Wired**, [s. l.], 16 nov. 2018. Available at: <https://www.wired.com/story/mcsweeneys-excerpt-the-right-to-experiment/>. Accessed on: 28 jun. 2023.

SCHWARTZ, Oscar. Untold History of AI: Algorithmic Bias Was Born in the 1980s A medical school thought a computer program would make the admissions process fairer—but it did just the opposite. **IEE Spectrum**, [s. l.], 15 apr. 2019. Available at: <https://spectrum.ieee.org/untold-history-of-ai-the-birth-of-machine-bias>. Accessed on: 18 oct. 2023.

SCHYNS, Camille. **The Lobbying Ghost in the Machine: Big Tech's covert defanging of Europe's AI Act**. [S. l.: s. n.], 2023. Available at: <https://corporateeurope.org/sites/default/files/2023-03/The%20Lobbying%20Ghost%20in%20the%20Machine.pdf>. Accessed on: 27 sep. 2023.

SCOTTISH SCHOOL PUPILS HAVE RESULTS UPGRADED. **BBC**, [s. l.], 11 aug. 2020. Available at: https://www.bbc.com/news/uk-scotland-53740588?intlink_from_url=https://www.bbc.co.uk/news/topics/c6n96k71wq0t/scottish-exam-results&link_location=live-reporting-story. Accessed on: 18 oct. 2023.

SEBRIAM, Debora; GONSALES, Priscila. **CIEB Estudos #2. Inovação aberta em educação: Conceitos e modelos de negócios**. [S. l.: s. n.], 2017. Available at: <https://estudocieb.educadigital.org.br/wp-content/uploads/2017/02/CIEB-Estudos-2-Inovacao-Aberta-em-Educacao.pdf>. Accessed on: 25 oct. 2023.

SEKI, Allan Kenji; VENCO, Selma Borghi. Política Nacional de Educação Digital: Uma análise de seus rebatimentos na educação pública brasileira. **Germinal: Marxismo e Educação em Debate**, [s. l.], v. 15, n. 2, p. 448–471, 2023.

SELWYN, Neil. Data entry: towards the critical study of digital data and education. **Learning, Media and Technology**, [s. l.], v. 40, n. 1, p. 64–82, 2015.

SELWYN, Neil; GAŠEVIĆ, Dragan. The datafication of higher education: discussing the promises and problems. **Teaching in Higher Education**, [s. l.], v. 25, n. 4, p. 527–540, 2020.

SHAH, Dhawal. By The Numbers: MOOCs in 2021. **The Report**, [s. l.], 1 dec. 2021. Available at: <https://www.classcentral.com/report/mooc-stats-2021/>. Accessed on: 30 jul. 2023.

SIEMENS, George *et al.* **Open Learning Analytics: an integrated & modularized platform proposal to design, implement and evaluate an open platform to integrate heterogeneous learning analytics techniques**. [S. l.: s. n.], 2011. Available at: <https://solaresearch.org/wp-content/uploads/2011/12/OpenLearningAnalytics.pdf>. Accessed on: 16 mar. 2023.

SIIBAK, Andra; MASCHERONI, Giovanna. **Children's data and privacy in the digital age**. Hamburg: [s. n.], 2021. Available at: https://www.ssoar.info/ssoar/bitstream/handle/document/76251/ssoar-2021-siibak_et_al-

Childrens_data_and_privacy_in.pdf?sequence=4&isAllowed=y&lnkname=ssoar-2021-siibak_et_al-Childrens_data_and_privacy_in.pdf. Accessed on: 30 dec. 2023.

SINGER, Natasha. How Google Took Over the Classroom. **The New York Times**, [s. l.], 13 mai 2017. Available at: [nytimes.com/2017/05/13/technology/google-education-chromebooks-schools.html](https://www.nytimes.com/2017/05/13/technology/google-education-chromebooks-schools.html). Accessed on: 14 aug. 2023.

SINGER, Natasha. How the Netherlands Is Taming Big Tech. **The New York Times**, [s. l.], 18 jan. 2023. Available at: <https://www.nytimes.com/2023/01/18/technology/dutch-school-privacy-google-microsoft-zoom.html>. Accessed on: 14 sep. 2023.

SINGH, Kishore. **Report of the Special Rapporteur on the Right to Education, Kishore Singh: protecting the right to education against commercialization. A/HRC/29/30**. [S. l.: s. n.], 2015a. Available at: <https://digitallibrary.un.org/record/797838>. Accessed on: 25 dec. 2023.

SINGH, Kishore. **Report of the Special Rapporteur on the right to education on Public Private Partnerships and the right to education. A/70/342**. [S. l.: s. n.], 2015b. Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/264/89/PDF/N1526489.pdf?OpenElement>. Accessed on: 1 nov. 2023.

SINHA, Shantanu. New education features to help teachers save time and support students. **Google - The Keyword**, [s. l.], 22 jan. 2024. Available at: <https://blog.google/outreach-initiatives/education/bett-2024-google-for-education-updates/>. Accessed on: 14 aug. 2023.

SINHA, Shantanu. New Google for Education tools for how you teach, learn and manage. **Google - The Keyword**, [s. l.], 22 jun. 2023. Available at: <https://blog.google/outreach-initiatives/education/google-for-education-iste-2023/>. Accessed on: 14 aug. 2023.

SIVON. **Over ons**. [S. l.], [s. d.]. Available at: <https://sivon.nl/over-ons/>. Accessed on: 27 sep. 2023.

SIVON. **Stand van zaken DPIA Google Workspace: update privacymaatregelen**. [S. l.], 2023. Available at: <https://sivon.nl/2023/04/stand-van-zaken-dpia-google-workspace-update-privacymaatregelen/>. Accessed on: 27 sep. 2023.

SKINNER, B. F. Teaching Machines: From the experimental study of learning come devices which arrange optimal conditions for self-instruction. **Science**, [s. l.], v. 128, n. 3330, p. 969–977, 1958.

SMUHA, Nathalie. Digital Sovereignty in the European Union: Five Challenges from a Normative Perspective. *In:* , 2023a. **Working paper - ERA Conference Proceedings**. [S. l.: s. n.], 2023.

SMUHA, Nathalie *et al.* **How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act**. [S. l.: s. n.], 2021. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991. Accessed on: 21 oct. 2023.

SMUHA, Nathalie. Pitfalls and pathways for Trustworthy Artificial Intelligence in education. *In: HOLMES, Wayne; PORAYSKA-POMSTA, Kaška (org.). The Ethics of Artificial Intelligence in Education: Practices, Challenges, and Debates.* [S. l.]: Routledge, 2023b.

SOLOVE, Daniel J. **Artificial Intelligence and Privacy.** 2024. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4713111. Accessed on: 6 feb. 2024.

SOLOVE, Daniel J. Murky Consent: An Approach to the Fictions of Consent in Privacy Law. **Boston University Law Review (Advance online publication)**, [s. l.], 2023. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4333743. Accessed on: 1 aug. 2023.

SOLOW-NIEDERMAN, Alicia. Information Privacy and the Inference Economy. **Northwestern University Law Review**, [s. l.], v. 117, n. 2, p. 357–424, 2022. Available at: <https://scholarlycommons.law.northwestern.edu/nulr/vol117/iss2/1>. Accessed on: 12 dec. 2023.

SORKIN, Andrew Ross; PETERS, Jeremy W. Google to Acquire YouTube for \$1.65 Billion. **The New York Times**, [s. l.], 9 oct. 2006. Available at: <https://www.nytimes.com/2006/10/09/business/09cnd-deal.html>. Accessed on: 8 aug. 2023.

SPECTOR, J Michael. **The SAGE encyclopedia of educational technology.** Thousand Oaks, California: SAGE Publications, 2015.

STANDAERT, Michael. Chinese primary school halts trial of device that monitors pupils' brainwaves. **The Guardian**, [s. l.], 1 nov. 2019. Available at: <https://www.theguardian.com/world/2019/nov/01/chinese-primary-school-halts-trial-of-device-that-monitors-pupils-brainwaves>. Accessed on 15 jan. 2014.

STATZ, Pamela. Google Announces Office Suite, Takes Aim at Microsoft. **Wired**, [s. l.], 28 aug. 2006. Available at: <https://www.wired.com/2006/08/google-announces-office-suite-takes-aim-at-microsoft/>. Accessed on: 8 aug. 2023.

STRAUSS, Valerie. Bill Gates: 'It would be great if our education stuff worked but...'. **The Washington Post**, [s. l.], 27 sep. 2013. Available at: <https://www.washingtonpost.com/news/answer-sheet/wp/2013/09/27/bill-gates-it-would-be-great-if-our-education-stuff-worked-but/>. Accessed on: 2 jul. 2023.

STRINGER, Eleanor; LEWIN, Cathy; COLEMAN, Robbie. **Using Digital Technology to Improve Learning: Guidance Report.** [S. l.: s. n.], 2019. Available at: https://educationendowmentfoundation.org.uk/public/files/Publications/digitalTech/EEF_Digital_Technology_Guidance_Report.pdf. Accessed on: 10 mai 2023.

SUJON, Zoetanya. Disruptive play or platform colonialism? The contradictory dynamics of Google expeditions and educational virtual reality. **Digital Culture & Education**, [s. l.], v. 11, n. 1, p. 1–21, 2019. Available at: <https://static1.squarespace.com/static/5cf15af7a259990001706378/t/5ebe94dcc4b8b2207a72b2e6/1589548261728/Cover-merged.pdf>. Accessed on: 10 aug. 2023.

SURF. **Agreement with Google on privacy risks.** [S. l.], 2021a. Available at: <https://www.surf.nl/en/agreement-with-google-on-privacy-risks>. Accessed on: 27 sep. 2023.

SURF. **Essential Services.** [S. l.], [s. d.]. Available at: <https://www.surf.nl/files/2023-07/bijlage-list-of-essential-services.pdf>. Accessed on: 27 sep. 2023 a.

SURF. **Google Workspace for Education support package.** [S. l.], 2021b. Available at: <https://www.surf.nl/en/google-workspace-for-education-support-package>. Accessed on: 27 sep. 2023.

SURF. **Privacy risks from 2021 Google Workspace for Education DPIA sufficiently resolved.** [S. l.], 2023a. Available at: Privacy risks from 2021 Google Workspace for Education DPIA sufficiently resolved. Accessed on: 27 sep. 2023.

SURF. **Status of Google Workspace DPIA: update on privacy measures.** [S. l.], 2023b. Available at: <https://www.surf.nl/en/status-of-google-workspace-dpia-update-on-privacy-measures>. Accessed on: 27 sep. 2023.

SURF. **SURF and SIVON discuss privacy risks with Google.** [S. l.], 2021c. Available at: <https://www.surf.nl/en/surf-and-sivon-discuss-privacy-risks-with-google>. Accessed on: 27 sep. 2023.

SURF. **SURF is the collaborative organisation for IT in Dutch education and research.** [S. l.], [s. d.]. Available at: <https://www.surf.nl/en>. Accessed on: 27 sep. 2023 b.

SURF. **SURF, SIVON and Google reach agreement Terms of Service Google Chrome.** [S. l.], 2023c. Available at: <https://www.surf.nl/en/surf-sivon-and-google-reach-agreement-terms-of-service-google-chrome>. Accessed on: 27 sep. 2023.

SURF; SIVON. **Final improvement plan Google ChromeOS and Chrome browser on Chrome devices.** [S. l.], 2023. Available at: <https://sivon.nl/wp-content/uploads/2023/07/Improvement-plan-Google-for-ChromeOS-on-managed-devices.pdf>. Accessed on: 27 sep. 2023.

SUSSER, Daniel; ROESSLER, Beate; NISSENBAUM, Helen. Technology, autonomy, and manipulation. **Internet Policy Review**, [s. l.], v. 8, n. 2, 2019.

SWIST, Teresa *et al.* **As more biometric data is collected in schools, parents need to ask these 10 questions.** [S. l.], 2022. Available at: <https://theconversation.com/as-more-biometric-data-is-collected-in-schools-parents-need-to-ask-these-10-questions-191263>. Accessed on: 27 jul. 2023.

TAEKEMA, Sanne. Theoretical and Normative Frameworks for Legal Research: Putting Theory into Practice. **Law and Method**, [s. l.], 2018. <https://doi.org/10.5553/REM/000031>.

TEFFÉ, Chiara Spadaccini de. Dados sensíveis de crianças e adolescentes: aplicação do melhor interesse e tutela integral. In: LATERÇA, Priscilla *et al.* (org.). **Privacidade e Proteção de Dados de Crianças e Adolescentes.** [S. l.]: Obliq Livros; ITS Rio, 2021. p. 342–395. Available at: <https://itsrio.org/wp-content/uploads/2021/10/Privacidade-e-Protecao-de-Dados-de-Crian%C3%A7as-e-Adolescentes-ITS.pdf>. Accessed on: 4 oct. 2023.

TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais de crianças e adolescentes: considerações sobre o artigo 14 da LGPD. *In*: MULHOLLAND, Caitlin (org.). **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélogo, 2020.

TEFFÉ, Chiara Spadaccini de; FERNANDES, Elora. Contratação em redes sociais e proteção de dados de crianças e adolescentes. *In*: ROQUE, Andre Vasconcelos; OLIVA, Milena Donato (org.). **Direito na era digital: aspectos negociais, processuais e registraes**. [S. l.]: Editora Jus Podivm, 2022. p. 97–122.

TERRA, Floor; NAS, Sjoera; ROOSENDAL, Arnold. **Inspection results Google Chrome for Education. SIVON**. [S. l.: s. n.], 2023. Available at: <https://sivon.nl/wp-content/uploads/2023/07/20230629-Chrome-inspection-report-v1-2-public-NEW.pdf>. Accessed on: 27 sep. 2023.

TERWANGNE, Cécile de. Article 5. Principles relating to processing of personal data. *In*: KUNER, Christopher; BYGRVE, Lee A.; DOCKSEY, Christopher (org.). **The EU General Data Protection Regulation: A Commentary**. [S. l.]: Oxford University Press, 2020a. p. 309–320.

TERWANGNE, Cécile de. Article 16. Right to rectification. *In*: KUNER, Christopher *et al.* (org.). **The EU General Data Protection Regulation: A Commentary**. [S. l.]: Oxford University Press, 2020b. p. 469–474.

THATCHER, Jim; O’SULLIVAN, David; MAHMOUDI, Dillon. Data colonialism through accumulation by dispossession: New metaphors for daily data. **Environment and Planning D: Society and Space**, [s. l.], v. 34, n. 6, p. 990–1006, 2016.

THE EDITORS OF ENCYCLOPAEDIA BRITANNICA. **Technology**. *In*: ENCYCLOPAEDIA BRITANNICA. [S. l.: s. n.], 2022. Available at: <https://www.britannica.com/technology/technology>. Accessed on: 19 mar. 2023.

THE EDUCATION COALITION. **History of Telecourses**. [S. l.], [s. d.]. Available at: <https://www.tecweb.org/eddevel/telecon/de92.html>. Accessed on: 16 mai 2023.

TIETOSUOJAVALTUUTETTU. **Tietosuojaaltuutetun päätös käsittelyn lainmukaisuutta ja henkilötietojen siirtoa kolmansiin maihin koskevassa asiassa**. [S. l.], 2021. Available at: <https://finlex.fi/fi/viranomaiset/tsv/2021/20211503?search%5Btype%5D=pika&search%5Bpika%5D=google>. Accessed on: 4 dec. 2023.

TOBIN, John; FIELD, Sarah M. Article 16. The Right to Protection of Privacy, Family, Home, Correspondence, Honour and Reputation. *In*: TOBIN, John (org.). **The UN Convention on the Rights of the Child: A Commentary**. Oxford: Oxford University Press, 2019. p. 551–599.

TOMAŠEVSKI, Katarina. **Human rights obligations: making education available, accessible, acceptable and adaptable**. [S. l.: s. n.], 2001. Available at: <https://www.right-to-education.org/resource/primer-no-3-human-rights-obligations-making-education-available-accessible-acceptable-and>. Accessed on: 11 jul. 2023.

TOSONI, Luca. Article 4(25). Information society service. *In*: KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher (org.). **The EU General Data Protection Regulation (GDPR): A Commentary**. [S. l.]: Oxford University Press, 2020. p. 292–302.

TRZASKOWSKI, Jan. Data-driven business models - Privacy and marketing. *In*: KOSTA, Eleni; LEENES, Ronald; KAMARA, Irene (org.). **Research Handbook on EU Data Protection Law**. [S. l.]: Edward Elgar, 2022. p. 206–239.

UNDERSTANDING DIGITAL CREDENTIALS BUILDING VALUE FROM AN ECOSYSTEM OF OPEN STANDARDS. [S. l.], [s. d.]. Available at: <https://www.imsglobal.org/understanding-digital-credentials>. Accessed on: 4 mai 2023.

UNESCO. **An ed-tech tragedy? Educational technologies and school closures in the time of COVID-19**. Paris: [s. n.], 2023a. Available at: <https://unesdoc.unesco.org/ark:/48223/pf0000386701>. Accessed on: 24 sep. 2023.

UNESCO. **Global Education Monitoring Report. Technology in education: A Tool in Whose Terms?** Paris: [s. n.], 2023b. Available at: <https://www.unesco.org/gem-report/en/technology>. Accessed on: 30 jul. 2023.

UNESCO. **Rethinking education: towards a global common good?** Paris: [s. n.], 2015.

UNESCO INSTITUTE FOR STATISTICS (UIS). **Guide to measuring information and communication technologies (ICT) in education**. [S. l.]: UNESCO Institute for Statistics, 2009. Available at: <https://unesdoc.unesco.org/ark:/48223/pf0000186547>. Accessed on: 29 jul. 2023.

UNICEF. **Convention on the Rights of the Child: For every child, every right**. [S. l.], [s. d.]. Available at: <https://www.unicef.org/child-rights-convention>. Accessed on: 5 jul. 2023.

UNICEF. **Early Warning Systems for Students at Risk of Dropping Out: Policy and Practice for Enrolling All Children and Adolescents in School and Preventing Dropout**. [S. l.: s. n.], 2018. Available at: https://www.unicef.org/eca/sites/unicef.org.eca/files/2018-11/Early%20warning%20systems%20for%20students%20at%20risk%20of%20dropping%20out_0.pdf. Accessed on: 12 nov. 2023.

UNICEF. **Implementation handbook for the Convention on the Rights of the Child**. [S. l.]: UNICEF, 2007. Available at: <https://www.unicef.org/reports/implementation-handbook-convention-rights-child>. Accessed on: 13 jul. 2023.

UNICEF. **Policy guidance on AI for children 2.0**. [S. l.: s. n.], 2021. Available at: <https://www.unicef.org/globalinsight/reports/policy-guidance-ai-children>. Accessed on: 30 jul. 2023.

UNICEF. **The State of the World's Children 2017: Children in a Digital World** Unicef. [S. l.: s. n.], 2017. Available at: <https://www.unicef.org/reports/state-worlds-children-2017>. Accessed on: 31 oct. 2022.

UNITED NATIONS HUMAN RIGHTS. OFFICE OF THE HIGH COMMISSIONER. **Guiding Principles on Business and Human rights. Implementing the United Nations**

“Protect, Respect and Remedy” Framework. HR/PUB/11/04. [S. l.: s. n.], 2011. Available at:

https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf. Accessed on: 9 jul. 2023.

UNITED NATIONS HUMAN RIGHTS TREATY BODIES. **Committee on the Rights of the Child.** [S. l.], [s. d.]. Available at: <https://www.ohchr.org/en/treaty-bodies/crc>. Accessed on: 30 dec. 2023.

UPSON, Linus. A new kind of computer: Chromebook. **Google Official Blog**, [s. l.], 11 mai 2011. Available at: <https://googleblog.blogspot.com/2011/05/new-kind-of-computer-chromebook.html?+>. Accessed on: 8 aug. 2023.

VAIDHYANATHAN, Siva. **The Googlization of everything (and why we should worry).** [S. l.]: University of California Press, 2011.

VANCE, Amelia; SEXTON, Morgan; KALPOS, Katherine Sledge. Tis the Season for Rulemaking: FTC Announces New COPPA NPRM. **Public Interest Privacy Center**, [s. l.], 20 dec. 2023. Available at: <https://pipc.substack.com/p/tis-the-season-for-rulemaking-ftc?r=26ap01>. Accessed on: 25 dec. 2023.

VARADAN, Sheila. The principle of evolving capacities under the UN convention on the rights of the child. **International Journal of Children’s Rights**, [s. l.], v. 27, n. 2, p. 306–338, 2019.

VEDDER, Anton. KDD: The challenge to individualism. **Ethics and Information Technology**, [s. l.], v. 1, p. 275–281, 1999.

VELIZ, Carissa. Digitization, Surveillance, Colonialism. **Liberties**, [s. l.], v. 3, n. 1, 2022. Available at: <https://libertiesjournal.com/articles/digitization-surveillance-colonialism/>. Accessed on: 31 oct. 2022.

VERDOODT, Valerie. **Children’s rights and commercial communication in the digital era: Towards an empowering regulatory framework for commercial communication.** [S. l.]: Intersentia, 2020.

VERTESI, Janet. My Experiment Opting Out of Big Data Made Me Look Like a Criminal. **Time**, [s. l.], 1 mai 2014. Available at: <https://time.com/83200/privacy-internet-big-data-opt-out/>. Accessed on: 24 jun. 2023.

VICENTINI, Letizia *et al.* **Future opportunities for education technology in England.** [S. l.: s. n.], 2022. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1080930/Future_opportunities_for_education_technology_in_England_June_2022.pdf. Accessed on: 19 oct. 2023.

VINCENT-LANCRIN, Stéphan. Frontiers of smart education technology: Opportunities and challenges. *In*: OECD DIGITAL EDUCATION OUTLOOK 2021: PUSHING THE FRONTIERS WITH ARTIFICIAL INTELLIGENCE, BLOCKCHAIN AND ROBOTS. Paris: OECD Publishing, 2021. p. 19–42.

VOGIATZOGLOU, Plixavra; VALCKE, Peggy. Two decades of Article 8 CFR: A critical exploration of the fundamental right to personal data protection in EU law. *In*: KOSTA, Eleni; LEENED RONALD; KAMARA, Irene (org.). **Research Handbook on EU Data Protection Law**. [S. l.]: Edward Elgar, 2022. p. 11–49.

VTC. **Aanbeveling VTC bij de Digisprong in het onderwijs**. [S. l.], 2021. Available at: <https://overheid.vlaanderen.be/digitale-overheid/digisprong-in-het-onderwijs>. Accessed on: 13 dec. 2023.

VTC. **Over de Vlaamse Toezichtcommissie**. [S. l.], [s. d.]. Available at: <https://overheid.vlaanderen.be/vlaamse-toezichtcommissie>. Accessed on: 14 dec. 2023.

VTC. **Standpunt VTC i.v.m. gebruik Google for Education door basis- en secundair onderwijs**. [S. l.: s. n.], 2023a.

VTC. **Vragen VTC aan Google na Overleg met Google en na Brief aan Minister van Onderwijs**. [S. l.: s. n.], 2023b. Available at: https://overheid.vlaanderen.be/sites/default/files/media/VTC/VTC_O_2023_01_vragen_aan_Google_deel_2_naVTC_def.pdf?timestamp=1689170403. Accessed on: 13 dec. 2023.

WACHTER, Sandra; MITTELSTADT, Brent Daniel. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. **Columbia Business Law Review**, [s. l.], n. 2, p. 494–620, 2019. <https://doi.org/10.7916/cblr.v2019i2.3424>.

WAGNER, Alan; BORENSTEIN, Jason; HOWARD, Ayanna. Overtrust in the robotic age. **Communications of the ACM**, NEW YORK, v. 61, n. 9, p. 22–24, 2018.

WALKER, Christopher. Unlocking the impact of edtech. **impactInvestor**, [s. l.], 15 dec. 2023. Available at: <https://impact-investor.com/unlocking-the-impact-of-edtech/>. Accessed on: 23 dec. 2023.

WATTERS, Audrey. **How Steve Jobs Brought the Apple II to the Classroom**. [S. l.], 2015. Available at: <http://hackededucation.com/2015/02/25/kids-cant-wait-apple>. Accessed on: 27 jul. 2023.

WATTERS, Audrey. School Work and Surveillance. **HackEducation**, [s. l.], 30 apr. 2020. Available at: <https://hackededucation.com/2020/04/30/surveillance>. Accessed on: 28 mai 2023.

WATTERS, Audrey. **Teaching Machines**. [S. l.]: The MIT Press, 2021.

WATTERS, Audrey. The Teleology of Ed-Tech. **oeb Insights**, [s. l.], 11 apr. 2019. Available at: <https://oeb.global/oeb-insights/the-teleology-of-ed-tech/>. Accessed on: 13 mai 2023.

WEBB, P. Taylor; SELLAR, Sam; GULSON, Kalervo N. Anticipating education: governing habits, memories and policy-futures. **Learning, Media and Technology**, [s. l.], v. 45, n. 3, p. 284–297, 2020.

WELLER, Martin. **25 Years of Ed Tech**. [S. l.: s. n.], 2020.

WELLER, Martin. **The Battle For Open: How openness won and why it doesn't feel like victory**. London: Ubiquity Press, 2014. Available at:

<https://library.oapen.org/bitstream/id/3b361bf2-c5e4-4bcd-8b69-3cdcbab008c5/533876.pdf>. Accessed on: 18 mar. 2023.

WELLER, Martin. **Virtual Learning Environments: Using, Choosing and Developing Your VLE**. New York: Routledge, 2007.

WEST, Sarah Myers. Data Capitalism: Redefining the Logics of Surveillance and Privacy. **Business and Society**, [s. l.], v. 58, n. 1, p. 20–41, 2019.

WHO WATCHES AI WATCHING STUDENTS? [AUDIO PODCAST EPISODE]. Apresentado por Jennifer Strong. [S. l.]: MIT Technology Review, 2022. Available at: <https://www.technologyreview.com/2022/06/29/1057103/podcast-who-watches-ai-watching-students/>. Accessed on: 5 mai 2023.

WILLIAMSON, Ben. Datafication of Education: A Critical Approach to Emerging Analytics Technologies and Practices. In: BEETHAM, Helen; SHARPE, Rhona (org.). **Rethinking Pedagogy for a Digital Age: Principles and Practices of Design**. 3. ed. [S. l.]: Routledge, 2019.

WILLIAMSON, Ben. Digital education governance: data visualization, predictive analytics, and ‘real-time’ policy instruments. **Journal of Education Policy**, [s. l.], v. 31, n. 2, p. 123–141, 2016.

WILLIAMSON, Ben. Google’s plans to bring AI to education make its dominance in classrooms more alarming. **Fast Company**, [s. l.], 28 mai 2021. Available at: <https://www.fastcompany.com/90641049/google-education-classroom-ai>. Accessed on: 14 aug. 2023.

WOLFF, Josephine; LEHR, William; YOO, Christopher, S. **Public Law and Legal Theory Research Paper Series Research Paper No. 23-32. Lessons from GDPR for AI Policymaking**. 2023. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4528698. Accessed on: 6 feb. 2024.

WOLFSON, Lisa. Venture Capital Needed for ‘Broken’ U.S. Education, Thrun Says. **Bloomberg**, [s. l.], 18 jun. 2013. Available at: <https://www.bloomberg.com/news/articles/2013-06-18/venture-capital-needed-for-broken-u-s-education-thrun-says#xj4y7vzkg>. Accessed on: 12 nov. 2023.

WOLVERS, Andrea *et al.* Introduction. In: CONCEPTS OF THE GLOBAL SOUTH: VOICES FROM AROUND THE WORLD. [S. l.]: Global South Studies Center, University of Cologne, 2015. p. 1–2. Available at: https://kups.ub.uni-koeln.de/6399/1/voices012015_concepts_of_the_global_south.pdf. Accessed on: 20 jun. 2023.

WP29. **Opinion 02/2013 on apps on smart devices**. [S. l.: s. n.], 2013. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf. Accessed on: 18 jul. 2023.

WP29. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.** [S. l.: s. n.], 2016. Available at: <https://ec.europa.eu/newsroom/article29/items/612053/en>. Accessed on: 27 oct. 2023.

WP29. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679.** [S. l.: s. n.], 2017. Available at: <https://ec.europa.eu/newsroom/article29/items/611236/en>. Accessed on: 19 jul. 2023.

WP29. **Guidelines on the right to “data portability”.** [S. l.: s. n.], 2017. Available at: <https://ec.europa.eu/newsroom/article29/items/611233>. Accessed on: 28 oct. 2023.

WP29. **Guidelines on transparency under Regulation 2016/679.** [S. l.: s. n.], 2018. Available at: <https://ec.europa.eu/newsroom/article29/items/622227/en>. Accessed on: 19 jul. 2023.

WP29. **Opinion 03/2013 on purpose limitation.** [S. l.: s. n.], 2013. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Accessed on: 18 jul. 2023.

WP29. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.** [S. l.: s. n.], 2014. Available at: http://ec.europa.eu/justice/data-protection/index_en.htm. Accessed on: 17 jul. 2023.

YOUNG, Andrew; VERHULST, Stephan G. Why we need responsible data for children. **The Conversation**, [s. l.], 23 mar. 2020. Available at: <https://theconversation.com/why-we-need-responsible-data-for-children-134052>. Accessed on: 24 jun. 2023.

ZANATTA, Rafael; VALENTE, Jonas; MENDONÇA, Julia. Entre o abusivo e o excessivo: novos contornos jurídicos para o tratamento de dados pessoais de crianças e adolescentes na LGPD. In: LATERÇA, Priscilla *et al.* (org.). **Privacidade e Proteção de Dados de Crianças e Adolescentes.** Rio de Janeiro: Obliq; ITS Rio, 2021. Available at: <https://itsrio.org/pt/publicacoes/privacidade-e-protecao-de-dados-de-criancas-e-adolescentes/>. Accessed on: 5 oct. 2023.

ZANFIR-FORTUNA, Gabriela. Article 21. Right to object. In: KUNER, Christopher *et al.* (org.). **The EU General Data Protection Regulation: A Commentary.** [S. l.]: Oxford University Press, 2020. p. 506–521.

ZEIDE, Elana. Robot Teaching, Pedagogy, and Policy. In: **THE OXFORD HANDBOOK OF ETHICS OF AI.** [S. l.]: Oxford University Press, 2020. p. 788–803.

ZHANG, Xinli *et al.* The metaverse in education: Definition, framework, features, potential applications, challenges, and future research topics. **Frontiers in Psychology**, [s. l.], v. 13, 2022.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.** New York: PublicAffairs, 2019. v. E-book.