

2020年7月14日、
バングラデシュのダッカのミルプールにある、
ユニセフが支援する青少年フレンドリー保健サービスの1つからサービスを受けている
16歳の少女Jさんは、
自宅から友人たちとオンラインゲームをプレイしている。

ロックダウン中、Jさんはほとんどの時間を本を読んだり、
家族を助けたり、テレビでニュースを聞いたり、
携帯電話でオンライン授業に参加したり、
青少年が健康上の問題を共有し、
無料のカウンセリングや投薬を受けられる衛星健康キャンプを訪れたりして過ごした。

クレジット: UNICEF/UN0506086/ポール*
(写真等は、 原版 (英語版) を参照してください)

章



ガバナンスと 規制

キーメッセージ

教育テクノロジー業界の監督不足により、子どもたちのプライバシー、安全、幸福が危険にさらされています。

教育テクノロジーの管理は政府にとっての課題です。

82%の国には、教育技術を担当する政府部門または機関があります。48%の国ではこの機能は教育省が主導しており、29%の国では教育省と別の省庁が主導しており、5%の国では別の省庁全体が主導している。

公的機関は私的主体を統治するのに苦労している。

民間主体に対する監督が欠如しているとの懸念が提起されている。インドでは2021年の政府勧告で、教育テクノロジーの購入を検討している国民に対し、欺瞞的なマーケティング戦略に惑わされないよう警告した。

プライバシー、安全性、幸福のリスクは規制される必要があります。

新型コロナウイルス感染症のパンデミック下で子どもたちに推奨された163の教育テクノロジー製品を分析したところ、89%が教育現場や授業時間外で子どもに関する情報を収集できた、あるいは実際に収集したことが判明した。

データ保護法はまだできたばかりです。

教育におけるデータプライバシーを法律で保証している国はわずか16%です。10か国をさらに分析したところ、この法律にもかかわらず、子どもの権利はいまだ保護されていないことが判明した。

学校は子供たちと教師に関する豊富なデータを収集していますが、データの使用に関する規制はほとんどありません。欧州連合では、公立学校は一般データ保護規則の対象となっており、データ保護責任者を任命する必要があります。

教育に適用される人工知能アルゴリズムは、不平等を再生産したり、拡大したりする可能性があります。米国では、99人の開発者を評価したところ、先住民族に関する誤検知率が最も高かったことがわかりました。

安全上のリスクを無視することはできません。

教育はサイバー攻撃の標的になることが増えています。米国では、45の学区でサイバー攻撃を受けた学校の数が2021年から2022年にかけてほぼ2倍に増加しました。

世界では、16%の国が教育に焦点を当ててネットいじめを防止し、それに対処するための法律を制定しています。そのうち38%は、新型コロナウイルス感染症のパンデミック以降にそうしました。

スクリーンやテクノロジーへの曝露は、子どもたちの健康に影響を与えます。

2歳から17歳までの子どもを対象とした分析では、画面を見る時間が長いほど幸福度が低下することが示されました。米国では、11歳から14歳の子供が1日あたり9時間をスクリーンで過ごしていると推定されています。新型コロナウイルス感染症の影響でレベルが上昇した。

スクリーンタイムに関する規制やガイドラインはほとんどありません。中国では教育省が、教育ツールとしてデジタル機器を使用する時間を全体の授業時間の30%に制限した。

いくつかの国では、学校での携帯電話やその他のテクノロジーの使用を禁止しています。

世界的に見て、学校での電話の使用を禁止する法律や政策を設けている国は4分の1未満です。

プライバシー上の懸念から、特定のアプリケーションの使用を禁止している場合もあります。ドイツの一部の州では、一般データ保護規則に準拠していないMicrosoft製品を禁止しています。

政府は教育テクノロジーを管理することが困難であると感じています.....	144
デジタル プライバシー、安全性、福祉は規制される必要がある	147
結論	158

デジタルテクノロジーは現代の社会と経済のインフラを提供します。その開発、普及、保守は、複数の政府部門間で調整する必要があります。情報通信技術 (ICT) 業界への関与は、透明性のあるプロセスを通じて具体的に明確に規定する必要があります。教育におけるデジタル技術の統合に関連して、ガバナンスの問題はさらに複雑になります。

政府はインフラストラクチャに関する決定を下し、教育学を慎重に検討する必要があります。教育機関は、学習者や教師の利益を最優先に決定を下すために、学習者や教師と相談する必要があります。

教育の公平性、包括性、質、効率に関する政府の目標は、教育テクノロジー業界の目標と必ずしも一致しているわけではありません。業界の利益志向は、不適切、不公平、非効率的、持続不可能な行為につながり、幸福を損ない、セキュリティを侵害し、個人情報を悪用し、さらには人権を侵害し、テクノロジーを教育に適用するメリットを否定します。日常生活におけるテクノロジー、特に人工知能 (AI) の存在感の増大により、教育を受ける権利と学校内外で差別を受けない権利の両方に注意を払うことが求められています (Holmes et al., 2022)。プライバシーの権利に関する特別報告者によると、教育プロセスは「教育が行われる場所や方法を問わず、プライバシーやその他の権利の享受を損なう必要はなく、またそうすべきではない」(国連人権理事会、2021年)。

“

政府の目標は教育テクノロジー業界の目標と必ずしも一致しているわけではありません

”

デジタル化により教育の構造、形態、提供方法がますます複雑になるため、このような巻き添え被害を防ぐことは世界中の規制当局にとって新たな大きな課題となっています。民主主義、人権、法の支配を効果的に保護し促進するには、国内および国際レベルでの多くの関係者間の協力、パートナーシップ、および共通の目標の確立が必要です。この章では、ユーザー、特に子供が教育テクノロジーを使用する際に確実に保護されるようにするためのガバナンスと規制に焦点を当てます。

政府はそれが困難であると感じています 教育テクノロジーを統治するために

教育省は、教育テクノロジーの利用のガバナンスにおいて、経済開発、インフラ、エネルギー、通信部門と協力する必要があります。各部門は、イノベーション、デジタル変革、データのストレージと使用などの問題に関して、異なるビジョン、目標、目標を持っている可能性があります。政府主体に加えて、特に官民パートナーシップを通じた民間主体の役割を明確にする必要がある。これには透明性と説明責任のメカニズムが必要です (Hillman, 2022a; Lingard and Sellar, 2013)。

教育省が常に主導権を握るわけではない 教育テクノロジーについて

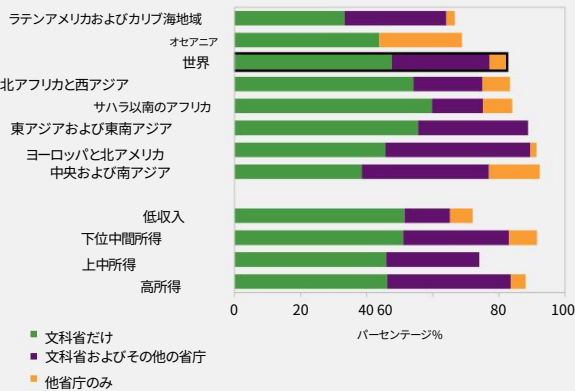
教育へのテクノロジーの統合を検討する場合、どの主体がそのプロセスを主導するのかを明確にすることが重要です。教育省はそのような決定を主導する必要があり、商業的な考慮事項よりも教育学的決定が優先される必要があります。教育テクノロジー企業が教育法の管轄下になく、純粋に商法によって判断される場合、学習者の最善の利益が危険にさらされる可能性があります。

この報告書の分析によると、82%の国で政府部門または機関がICTまたは教育技術を担当しており、48%の国では教育省が主導し、29%では教育省と別の省庁が主導している。そして5%では別の省庁がリーダーとなっています(図 8.1)。アルメニアでは、2009年の一般教育法により、教育におけるテクノロジーの導入と開発の責任は教育、科学、文化、スポーツ省に置かれています。

同省傘下の国立教育技術センターは、ICT導入、教師研修、教育におけるICT統合、データ収集の分野でさまざまな責任を負っている。

図 8.1:

10 か国中 6 か国で教育省が政府の教育技術機関を主導
教育テクノロジーを担当する政府部門または政府機関がある国の割合 (主要省庁別、2022 年)



GEM StatLink: https://bit.ly/GEM2023_fig8_1

出典: Profiles Enhancing Education Reviews (PEER)。

他の国では、他の省庁がより強い役割を担っています。

バングラデシュでは、初等教育と初等教育以降の教育を担当する2つの省庁がそれぞれ、カリキュラム、インフラストラクチャ、遠隔学習を含む教育におけるICTの調整と導入について責任を共有しています(バングラデシュ教育省、2013)。しかし、政府には、国家ICT戦略と政策開発、教育を含むさまざまなセクターにおけるICTの統合を担当する副大臣と首相のICT顧問からなるICT部門もある(バングラデシュICT部門、2023)。

ICT部門はまた、サイバーセキュリティ法と政策を主導し、デジタルセキュリティ庁(バングラデシュデジタルセキュリティ局、2023年)と協力してそれらの施行を確実にします。最後に、科学省と

テクノロジーは、その分野の教育機関もサポートしています(バングラデシュ科学技術省、2019)。

ケニアでは2019年に情報通信技術省が国家情報通信技術政策を発表し、eラーニングの取り組みにリソースを動員するための官民パートナーシップの促進などを通じ、教育のあらゆるレベルでICTを統合することを目指した。教育省は同年にデジタル経済青写真に貢献しました。ニジェールでは、教育テクノロジーのガバナンスは郵便・新情報技術省と教育省の間で共有されています。後者の中で、情報技術推進部門は、ハードウェアの選択、情報システムのセキュリティ、戦略的意思決定のためのデータ収集、教育におけるICTの統合を担当します。2017年以降、国立情報社会庁は、学校マッピングなどのICTプログラムの実施にも関与しています。パレスチナでは、電気通信・情報技術省と教育・高等教育省という2つの省庁が教育におけるICTの統合に責任を共有しています。ただし、どちらにも専門のICT部門はありません。

専門のタスクフォースまたは運営委員会は、ICT戦略の優先順位の質と一貫性をサポートし、その実施を調整します(Chuang et al., 2022)。

ブータン教育ブループリント2014~2024では、ICTプロジェクトの実施を推進する専用のガバナンス構造の必要性が強調されています。iSherig-2マスタープラン2019~2023では、教育におけるICTに関連するすべての事項を監督する部門と、教育、情報通信、財務省の代表者と実施機関のプロジェクトリーダーで構成される運営委員会の設立が推奨されています。ネパールでは、教育におけるICTマスタープラン2013~2017に基づいて2つの委員会が設立されました。政策決定を担当する運営委員会と、マスタープランの全体的な計画と部門間および政府機関間の調整を担当する調整委員会です。

高所得国では、デジタル教育のガバナンスと、政策設計、実施、監視におけるさまざまな利害関係者の代表を強化するメカニズムが出現しています。オーストラリアでは、広範な公開協議によりデジタル戦略の策定が進められてきました(オーストラリア人権委員会、2021年)。ヨーロッパでは、欧州委員会が主催するデジタル教育関係者フォーラムが、デジタル教育行動計画の実施におけるデジタル教育コミュニティの関与を促進してきました。

(欧州委員会、2022)。米国では、非営利団体である州教育技術ディレクター協会が、デジタル学習における公平性を擁護するフォーラムを提供しています。2016年国家教育技術計画は、教育者、イノベーター、研究者の協力から生まれ、フィードバックを提供し、235の模範的なプログラムと取り組みを特定しました。そのうち53は含まれています。この計画の原則と例は、「Every Student Succeeds Act」(米国教育技術局、2016年)のテクノロジーの効果的な使用をサポートする活動と一致しています。

しかし、2022年時点では、テクノロジーに関する計画や戦略的な会議に定期的に参加していることに同意した教育セクターのリーダーはわずか41%でした(SETDA、2022)。

“

専門のタスクフォースまたは運営委員会が、ICT戦略の優先順位の質と一貫性をサポートします

政府当局は統治に苦戦している
民間業者とのパートナーシップ

政府は、政府機関間の調整という課題とは別に、民間サプライヤーとの関係を管理するためのガバナンスメカニズムを確立するという新たな大きな課題に直面しています。接続、デバイス、ソフトウェア、コンテンツの取得と維持には費用がかかります。供給を拡大したい政府は民間企業の支援を求めることがよくあります。パートナーシップには、技術的専門知識、リースおよび契約サービス、トレーニング、機器およびソフトウェアライセンスの現物寄付などのインプットが含まれます(Pillay and Hearn、2011)。

アルゼンチンでは、教師によるICTカリキュラムと教材の開発を支援するために設立された公開会社 Educ.ar が、2000年に民間の寄付によって設立されました。2010年以降、同社は Conectar Igualdad (平等の接続) プログラムに向けた学校インフラの準備状況を監督し始めました(Roddisら、2021)。フランスでは、教育テクノロジー企業が、Territoires numériques éducatifs (デジタル教育地域) に基づいて、コンピュータ、インタラクティブスクリーン、ホワイトボード、スピーカー、Wi-Fi ホットスポット、安全なネットワークなどのリソースを学校に提供しました(Razquin et al.、2023)。インドネシアでは、教育テクノロジー企業が学生にサービスを提供しており、多くの場合、学生が認定教育プロバイダーになることを許可する政府とのライセンス契約に基づいており、ユーザーはプラットフォームへのアクセスに料金を支払います(Razquin et al.、2023)。サウジアラビアの Aanaab は、オンラインおよび教育における教師の専門能力開発を提供する教育テクノロジー企業です。

教育機関との協力を開始し、1,000人を超える教師を研修しています。教師は無料で登録できますが、トレーニング証明書を受け取るには料金を支払う必要があります(Razquin et al.、2023)。

主要な決定への非国家主体の参加を合理化する試みがいくつか行われてきた。

European EdTech Alliance は、政策や新興企業への支援を通じて「教育テクノロジーの国内外の成長を支援する」ことに取り組んでいる2,600を超える教育テクノロジー組織を結集しています。持続可能な官民パートナーシップのビジョンを策定し、「デジタル教育エコシステムのあらゆるレベルでの協力の範囲と境界を決定する、明確に定義されたフレームワークアーキテクチャ」を求めています(European EdTech Alliance、2022)。

しかし全体として、公的機関と大手テクノロジー企業との提携は、企業に不当な利益を与え、最終的には監視を損なう可能性があるため、しばしば議論を醸成している。

このようなパートナーシップに関しては、3種類の懸念が提起されています。1つ目は、生成されたデータの使用によるプライバシーと安全の侵害についてです。一部のテクノロジー企業はデータを独占しており、データの悪用に対する懸念が生じています。ブラジルでは、アマゾン、グーグル、ファーウェイ、マイクロソフト、オラクルなどの大手民間教育テクノロジーベンダーが教育省と緊密なパートナーシップ契約を結び、自社のソフトウェアへの無料アクセスを提供しようとしている。しかし、異なるベンダーの製品の使用を統合するのは簡単ではない可能性があるため、そのような契約では学生や教師に特定のソフトウェアの使用を強制する可能性もあります(Foditsch、2023)。Apple、Google、Microsoft は、ハードウェア(Chromebook、iPad、Surface など)とオペレーティングシステム(ChromeOS、iOS/

MacOS、Windows)を介してユーザーに関する情報を収集し、これらの攻撃者に一定のデータパイプラインを提供します。

複雑なデータパイプラインではガバナンスが非常に困難になる可能性があります(Chitkara、2022)。米国カリフォルニア州は2019年に「既存の教育、労働力、財政援助、社会福祉情報を結び付け、政策立案者、教育者、国民が機会格差に対処し、成果を向上させるための備えを強化する」ことを目的とした「Cradle-to-Career Data System Act」を承認しました。州全体のすべての学生に(California Data System、2019)。

この法律は、さまざまなパートナーからのデータの統合を義務付けており、その中には商用のものも含まれます(DXtera、2023年、Ed 3.0 Network、2020年、T3 Innovation Network、2023年)。ただし、これがガバナンスに及ぼす影響は精査されており、データシステムが公平かつ非差別的な方法で管理されることを保証する方法が問われています(EdTrust-West、2019; Moore、2020)。

2 番目の懸念は、プラットフォームの使用が必須の教育機能に及ぼす影響に関するものです。このようなプラットフォームは、教師が使用したいツールを選択する代わりにプラットフォームの使用を強制するため、教師の自主性を低下させる可能性があります。利益を追求するテクノロジープロバイダーの利益に合わせて生徒の評価を変更することができます。また、ビッグデータ分析に適合する方法で教育を定義し、コンテンツを形成し、意図した学習成果とその測定を行うこともできます。徐々に、長い間教師に委ねられてきた基本的な教育上の決定の管理は、カリキュラムや教科書の決定を特徴づけてきた精査や議論がなくなり、公共の領域から私的な領域へと移ってきた (Zeide, 2017)。

教育的にも適切な解決策を得るには協議が必要です。ドイツでは、非営利団体 Bündnis für Bildung (教育同盟) が連邦、地方、自治体レベルの教育当局と教育業界を結集させ、デジタル教育の課題に対する共同ソリューションを開発しています。

作業グループは、コンテンツ、プライバシー、学校改革、教師研修などの問題について活発に活動しています (Bündnis für Bildung, 2022)。

“

無料のコンテンツを提供する多くの教育テクノロジー企業が採用しているビジネス モデルは、欺瞞的なマーケティング戦略である可能性があります

”

3 番目の懸念は、消費者が誤解される可能性があるため、より伝統的な市場ガバナンスが必要であるということです。しかし政府は、教育テクノロジー企業を認定し、品質を保證することが難しいと感じています。政府による教育テクノロジー製品の購入はさておき、適切な品質基準、基準、評価が存在しないことは、教育テクノロジー製品を個人消費者に販売する場合にも問題となります (Patel et al., 2021)。無料のコンテンツを提供する多くの教育テクノロジー企業が採用しているビジネス モデルは、購読料の支払いを必要とする欺瞞的なマーケティング戦略である可能性があります。インドでは、学校教育・識字省が2021年に教育テクノロジー製品を購入する前に注意を払うよう国民に促す勧告を発行しました (インド教育省, 2021年)。

教育テクノロジー業界の対応の 1 つは自主規制でした。業界団体であるインドインターネット・モバイル協会の下にインド EdTechコンソーシアムを設立した。しかし、自主規制は明確な長期目標がなければ成功しません (Thathoo, 2022)。2022 年、消費者庁長官はコンソーシアムに対し、

「コミュニケーションと広告における非倫理的な行為を阻止するため」の広告ガイドラインを作成するための共同作業グループ (Press Trust of India, 2022)。

デジタル プライバシー、安全性、幸福は規制される必要がある

デジタル技術は教育と学習の優れた機会を提供しますが、著作権を含め、プライバシー、安全性、幸福に関連するリスクも伴います (ボックス 8.1)。教育の一環としてのインターネットの使用を含むインターネットは、ユーザーを個人データの悪用、プライバシーの侵害、悪用、個人情報の盗難、攻撃的なメッセージと画像、ネットいじめ、詐欺、フェイクニュースと誤った情報にさらしています (Smahel et al., 2020)。こうしたリスクにさらされている子どもたちは、その脆弱性や潜在的な損害の点でより大きな懸念を抱えています。

一方、デジタル機器の過度の使用は、身体的および精神的健康に悪影響を与える可能性があります。

プライバシーは日常的に侵害されています 私的利益

教育テクノロジー製品の製造を含むデジタル テクノロジー プロバイダーは、機密情報を含むユーザーに関するデータを収集し、保存します (Hillman, 2022)。したがって、教育と学習にテクノロジーを統合すると、生徒のプライバシーが侵害される可能性があります。学生データは、教育テクノロジー企業や広告テクノロジー企業によってマーケティング目的で使用されるべきではありません (国連人権理事会, 2022)。

しかし、新型コロナウイルス感染症のパンデミック下で子どもの学習に推奨された163の教育テクノロジー製品を分析したところ、89%が教育現場や授業時間外に子どものフォローをすることができた、あるいは実際にフォローしたことが判明した。学習プラットフォームにインストールされた追跡テクノロジーは、子供に関するデータを収集し、行動広告で子供をターゲットにするサードパーティ企業 (通常は広告テクノロジー会社) に送信しました。ほとんどの場合、監視はオプトアウトの機会もなく、子供やその親の同意もなしに行われました。パンデミック中に子供たちにオンライン教育を提供した42の政府のうち、39の政府は、子供の権利を「危険にさらす、または侵害する」方法でデジタルテクノロジーを使用しました。これらの国の中で、モロッコだけが、子どもの権利を損なう可能性のある教育テクノロジー製品を一切支持しなかった (ヒューマン・ライツ・ウォッチ, 2022)。

プライバシーの権利は、一般に、プライバシー、家族、家庭、通信への恣意的または違法な干渉、および名誉や評判に対する違法な攻撃から法律によって保護されるものとして枠付けされており、国際法を通じて人権として認識され、保護されています。

ボックス 8.1:

知的財産権の問題に対処する必要がある

デジタル技術によってコンテンツへのアクセスが拡大するという当初の期待は薄れてきました（第3章）。しかし、学校や教師は通常、知的財産を使用したり作成したりするため、所有権や、生徒や教師の作品の再利用や共有に対する制限について疑問が生じます。ヨーロッパ15か国での調査では、これらの問題が不明瞭であるか、対処されていないことが多いことが示されました。教育教材の著作権状況は作品の種類によって異なります。オンラインで無料で利用できるリソースは原則として教室で使用できますが、制限がある場合があります（Nobre, 2017）。欧州連合では、著作権で保護された作品を公衆に伝達する権利は原則的に調和されています（Nobre, 2017; Torres and Xalabarder, 2020）。欧州連合司法裁判所による4つの基準は、コミュニケーションの公共的で非営利的な性質と教育目的での使用を確立するために使用できます（EUIPO, 2022）。

知的財産および知的財産権に関連して教育に言及している18か国の法律をレビューしたところ、教育は主に著作権に関連しており、多くの場合高等教育機関を対象としていることが示唆されています（WIPO, 2022）。しかし、特にデジタル教育および学習ツールの使用が増加している中で、より幅広い問題に対してより明確な規制が必要です。たとえば、教師や生徒が作成したコンテンツに関する知的財産の所有権や、電子メール、クラウド、チャットルームを介して教育目的でコンテンツを共有する場合の法的立場などをカバーすることができます。オーストラリアのビクトリア州では、知的財産政策により、知的財産の所有、管理、使用の枠組みが規定されています。教育省は、州の政策および法律に従って知的財産を管理および使用します（ビクトリア州教育省, 2021a）。同局は、学校や教師に対し、著作権で保護された素材の使用と共有について指導しています。たとえば、教師は、教育部門またはその他の政府部門が所有し、クリエイティブ コモンズ ライセンスの対象となる著作権で保護された素材を使用できます（ビクトリア州教育省, 2021b）。

Bangladeshでは、新型コロナウイルス感染症以降の国家 ICT ロードマップにより、適切な暗号化を確保し、オンライン教育プロバイダーを保護するための知的財産権ポリシーの更新がサポートされました。シンガポールでは、教育省の教育者向け eMedia チャネルが、教師が自分や生徒が作成したビデオ プロジェクトや授業を共有するスペースを提供しています。アクセスは、適切なログイン情報を持つ教育者に限定されます。

2015年の欧州教育省の調査では、知的財産に関する研修は15か国で国の教育計画の優先事項ではなく、6か国では教師研修の一部ではないことが示されました（Office for Harmonization in the Internal Market, 2015）。

創造性、革新性、起業家精神、保護された教材の倫理的使用が知識と行動に影響を与えることができるように、教育における知的財産に対する共通のアプローチを開発するために、教育省と知的財産局の代表者からなる専門家ネットワークが形成されました。このネットワークは学校や教員養成大学と協力して、教育における知的財産問題についての意識を高めています（EUIPO, 2022b）。 Ideas Powered@Schools イニシアチブは、知的財産の価値とその尊重の重要性について生徒の意識を高めることを目的とした教育資料を作成および配布しています（EUIPO, 2022a）。

（教育への権利イニシアチブ, 2023）。しかし、デジタル技術によるプライバシーへの脅威は、法律専門家にとって新たな領域です。このようなプライバシー侵害による被害を定義するのはさらに困難です。それは未来にまで広がっていきます。その悪影響は、たとえ一人の個人にとっては最小限であったとしても、多くの人々に広がります。個人にとっては不便だけかもしれませんが、企業にとっては大きなメリットをもたらします。これらすべての要因は、裁判所の伝統的な危害に対する理解に疑問を投げかけています。法律専門家は、新たな状況を受け入れ始めたばかりです（Citron and Solove, 2022）。

テクノロジーを使用している間は生徒のプライバシーを保護すると同時に、学習をパーソナライズし、研究を進め、生徒の進歩を視覚化するためにデータを適切に使用できるようにする必要があります。学校は誰が生徒のデータにアクセスできるのかを認識し、生徒が学校でテクノロジーを使用するときに収集されるデータの種類を家族に開示する必要があります。学校は両親が両方とも安心していることを確認する必要があります。

また、学生はデータの収集と使用に関する自分の権利と責任を認識し、理解しています（ユネスコ, 2022）。

2021年、プライバシーの権利に関する国連特別報告者の報告書は、国の法的枠組みにおいて子どものプライバシーの権利が保護されていないこと、ベンダーのプライバシー取り決めに異議を申し立てたり、データの提供を拒否したりする親や子どもの能力の欠如を強調した。そして、学校が教育テクノロジーの選択に関連するプライバシーの問題に対処していないという事実。同報告書は、企業が思考特性、学習軌跡、エンゲージメント、応答時間、読んだページ、閲覧したビデオ、デバイスの識別や位置に至るまでのデータを広告パートナーなどの第三者と共有して「子どものデジタル教育記録を定期的に管理」していると指摘した。オンライン教育のための適切な法的枠組みを求めた（国連人権理事会, 2021年）。

2022年、教育の権利に関する国連特別報告者の報告書は、教育のデジタル化が「教育における他の人権、特にプライバシーの権利の侵害につながるべきではない」と強調した。それは、「テクノロジーを決定する人々とユーザーの間の力、意識、知識における大きな不均衡」についての懸念を引き起こした。また、データの収集と使用に関連する透明性の欠如、データに基づく意思決定に対する責任の範囲が不明確であること、正当な懸念に直面してもプライバシーの取り決めに異議を唱えることができないこと、学生のデジタル記録が悪影響を与える可能性があることにも注意を喚起しました。彼らの雇用の選択肢に影響を与える。

この報告書は各国に対し、複雑なオンライン環境における子どもの最善の利益を保護する子ども特有のプライバシーおよびデータ保護法を採択し、施行するよう求めた。プライバシーとデータ保護法によってあらゆる教育現場の成人を保護する。そして、教育現場、特に子供から決して収集すべきではない機密個人データのカテゴリを定義すること（国連人権理事会、2022年）。これらの懸念の一部はAIによってさらに高まります(ボックス 8.2)。

2021年、欧州評議会は、子どもの最善の利益、子どもの能力の発達、意見を聞く権利、差別されない権利という4つの基準に基づいて、教育現場における子どものデータ保護に関するガイドラインを発行しました。(ヨーロッパ、2021)。

データ保護法はまだ始まったばかりです

緊急の必要性があるにもかかわらず、教育におけるテクノロジーの使用におけるデータのプライバシーとセキュリティについては、国内法がほとんど取り上げていません。いくつかの例外を除いて、データ保護基準、消費者保護法、プライバシー規制は依然として断片的かつ不透明であり、生徒や教師に対する一貫性やプライバシーポリシーの妨げとなっています(教育への権利イニシアチブ、2023)。このレポートのPEER諸国プロファイルの分析では、教育におけるデータプライバシーを法律で保証している国は16%にすぎず、政策で保証している国は29%であることが示されています(これらの国は主にヨーロッパと北アメリカにあります)。41%の国では、新型コロナウイルス感染症のパンデミック以降、これらの政策が採用されています(図 8.2)。これについて10か国をさらに分析すると、

“

このレポートのためのPEER諸国プロファイルの分析によると、教育におけるデータプライバシーを法律で保証している国はわずか16%、政策で保証している国は29%であることが示されています。

”

報告書は、データのプライバシーと安全性を保護する法規定がある場合でも、データのプライバシーとセキュリティに対する子どもの権利に関する国際人権法が国家レベルで完全に施行されていないことを示唆しています(教育への権利イニシアチブ、2023年)。

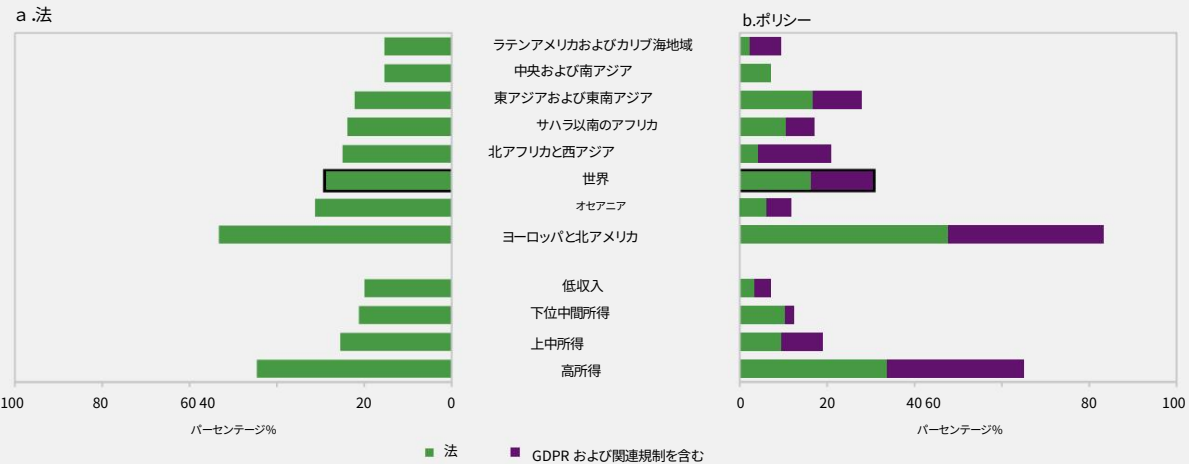
欧州連合では、2016年に発行され、2018年に発効した一般データ保護規則(GDPR)により、児童保護の法的状況が変わりました。第8条では、子供の個人データの処理は「子供が16歳以上である場合には合法であるものとする」と規定しています。16歳未満の子供の場合、同意は「親の責任を負う者」によって与えられた場合のみ合法となります。加盟国は年齢の引き下げを提案することができますが、13歳未満であってはなりません(欧州議会および欧州連合理事会、2016年)。

フランスでは、データ保護法第45条に従って、親権者は15歳までの子供の同意を共同で与える必要があります(フランス議会、2018年)。欧州以外でGDPRまたはその規制に準拠する法律を批准している国を加えると、少なくとも公立学校においてデータ保護を保証する国の割合は16%から31%に増加します。2018年にGDPRを施行するデータ保護法を可決したアイルランドでは、データ保護委員会が児童データ処理に関する14の中核原則を概説しました(アイルランドデータ保護委員会、2021)。

適切なレベルのデータ保護を保証している他の国には、アルゼンチン、中国、イスラエル、日本、ニュージーランド、韓国、英国、ウルグアイなどがあります。中国の法的枠組みは、教育環境などでの個人情報の共有に関して、子どものプライバシーを強力に保護しています。未成年者の保護と子供の個人情報の保護に関する2つの法律が、子供のデジタル権利に特化しています(中国サイバースペース管理局、2021年)。2021年、学校による未成年者の保護に関する規定は、教育におけるデジタル機器の使用における児童の保護を規制し、公平性、包摂性、尊厳の尊重、教育を受ける権利の原則も明記した(中国教育省、2021年)。日本では、青少年の安全で安心なインターネット利用のための環境整備強化法は、インターネットリテラシーの向上と、コンピュータやスマートフォンでのインターネットフィルタリングソフトウェアの使用を促進することを目的としています(日本政府、2008年)。ラテンアメリカでは、ほとんどの憲法が個人データ保護の権利を認めています。しかし、これらの権利を保護するための個別の規制は不足しています。GDPRはいくつかの取り組みを引き起こしました。コロンビアとメキシコは新しい法律を策定中です。

図 8.2:ほとんどの国

は教育におけるデータプライバシーを法律で保証していない 教育におけるデータ保護を保証している国の割合 (ツール別,2022年)



GEM StatLink: https://bit.ly/GEM2023_fig8_2
 出典: Profiles Enhancing Education Reviews (PEER)。

米国には、独立したデータ当局とデータ保護法があります。13歳未満の子供のデータ収集は児童オンライン プライバシー保護法によって規制されており、児童インターネット保護法は学校や図書館でインターネット上のわいせつまたは有害なコンテンツから子供を保護することを目的としています。保護者、生徒、学校職員は、誤用の結果を説明した書面による同意書、責任ある使用ポリシーに署名する必要があります。児童インターネット保護法は、学業上の誠実性の基準と、学校提供のデバイスまたは学校ネットワークを使用する際に生徒がアクセスできる、またはできないリソースも対象としています (米国教育省,2017年)。

しかし、これらすべての対策にもかかわらず、適切なデータ保護は保証されていません (教育への権利イニシアチブ,2023)。

インドでは、2021年にインド広告基準評議会が受け取った約5,500件の苦情のうち、3分の1が教育分野に関するものでした (Financial Express,2022)。広告と実際の製品との相違は虚偽広告に相当します (Varshney,2018)。消費者問題省は、一部の企業によるコースの不正販売疑惑に注目した (ET Online,2022)。

同団体は、最大手の教育テクノロジー新興企業の1つであるByju'sに対し、同社の広告内での主張を是正するために評議会と協力するよう勧告した。複雑な価格設定と財務契約、および積極的なマーケティングと販売戦略について懸念が生じています (Inamdar,2021)。

オマーンでは、2022年個人データ保護法により、個人データはのみ処理されるべきであると定められています

データ所有者の明示的な書面による同意がある場合。学校での教育用デバイスの使用に関する2022年の参照フレームワークでは、学校でのデバイスの使用に関連してデータ プライバシーを保護するためのセキュリティ規制のセクションが設けられました (オマーン教育省,2022)。2020年のアフリカでは、53か国中24か国が個人データを保護するための法律と規制を導入していました (PrivacyInternational.org,2020)。

学校は生徒、家族、教師に関する多くのデータを収集しますが、その中には生徒の生体認証データや健康データ、宗教に関する推測に使用できる食事要件など、機密データも含まれます。

ヨーロッパでは、公立学校はGDPRの「公的機関」として扱われています。企業は、収集したデータに対してより責任を負うデータ保護担当者を任命する必要があります。データが第三者によって扱われる場合、学校はデータがGDPRに準拠していること、および取引が法的拘束力のある契約内で行われることを確認する必要があります。データ主体に悪影響を与えるデータ侵害は、72時間以内にデータ保護当局に報告する必要があります。GDPRは、そのようなデータをいつどのように合法的に処理できるかについても決定します。たとえば、学校にはデータを処理する法的根拠があり、この作業は公共の利益にかかっています。

しかし、そうであっても、データを別のタスクに再利用することはできません。学校が生徒のデータを共有したい場合は、保護者または生徒の同意を得る必要があります。

“ 学校が生徒のデータを共有したい場合は、保護者または生徒の同意を得る必要があります ”

ボックス 8.2:

人工知能はプライバシーにさらなるリスクをもたらす

教育における人工知能 (AI) の使用は、管理プロセスやタスクの自動化から、カリキュラムやコンテンツの開発、指導、学習に至るまで、指数関数的に拡大しています。しかし、人工知能の倫理に関する2021年のユネスコ勧告は、教育と研究に特化したセクションであり、これは世界規模での初めての勧告であり、有形および無形のリスクについて記述されており、倫理的監視とともに堅牢な政策と法的枠組みが求められている(ユネスコ、2021年)。

AI は主に機械学習アルゴリズムに基づいており、人々の生活に大きな影響を与える可能性のある意思決定を行うために使用されます。アルゴリズムは公平で客観的であるとは程遠く、開発者のバイアスがかかっており、特に差別の点で不平等を再生産したり深めたりする可能性があります (欧州連合基本的権利庁、2022)。公平性の問題は、長い間評価における課題であり (Hutchinson and Mitchell, 2019)、信頼できる AI に関する国際機関の中核原則の 1 つに含まれています (欧州委員会、2019; OECD, 2019)。

アルゴリズムは、健康、司法、労働市場などのさまざまな領域に適用され、教育にも適用され、たとえば、学生の入学 (Engler, 2021) や中退率の予測 (Sybol et al., 2023) や成績の予測 (Yac, 2022) などに利用されています。新型コロナウイルス感染症 (COVID-19) の影響で英国で試験が中断されなければならなかったとき、スコアを予測するためにアルゴリズムが使用されたが、これは重大な結果をもたらした。

公立学校の生徒の成績は予想よりも低く、小規模な私立学校の生徒よりも低く、このような予測システムの責任と倫理について大きな疑問が生じています (Kolkman, 2020)。AI は生徒の実際の経験や背景を考慮しておらず、性別、人種、その他の偏見を示しています (Baker and Hawn, 2022; Borgesius, 2018; Buolamwini and Gebru, 2018)。

顔認識システムは、特定の人種に対して偏ることもあります (Garvie および Frankle, 2016)。米国で99人の開発者による189のソフトウェアアルゴリズムを評価したところ、白人の画像に比べてアジア系とアフリカ系アメリカ人の誤検知率が「個々のアルゴリズムに応じて10~100倍」高いことが判明した。偽陽性率が最も高いのは先住民族に関するものでした (NIST, 2019)。ブラジルでは、生徒の出席状況を監視する目的で、学校などの公共サービスへのアクセスを監視するために顔認識が使用されています。ただし、プログラムは他の情報を収集し、プライバシーを犠牲にして排除され疎外されたグループに関する情報を監視および記録することができます。最近承認されたデータ保護法は、公安目的でのデータ処理を対象としていないため、これらのシステムは、すでに脆弱なグループをプロファイリングし、処罰するために使用される可能性があります (Canto, 2021)。

米国テキサス州では、少なくとも 8 つの学区が顔認識を使用しており、これは法執行の目的でも使用されています (Simonite および Barber, 2019)。彼らは、システムが「ポーとして居眠りしている、携帯電話で遊んでいるなどの生徒の行動も認識できる」と主張して、教室に入り出すすべての生徒を識別できる学校での顔認識システムの使用を正当化している (ジン、2019)。中国サイバースペース局と教育省は2019年、AIを搭載したカメラやヘッドバンドを生徒が使用する前に保護者の同意を求め、データの暗号化を義務付ける規制を導入した (ユネスコ、2021年)。

多くの国では、子供の個人情報をいつどのように共有することが合法であるかについての具体的な規制はまだありません。データ処理に対する同意は、教育上必要な場合、または同意の根拠を理解していない場合、子供や親が拒否できない場合があるため、要求されても無効となる場合があります (欧州データ保護委員会、2020)。

既存の同意基準が学校に適用されるかどうかについては混乱が生じる可能性があります。英国では、情報コミッショナー局が、子供がアクセスする可能性が高いオンライン サービスに適用される、年齢に応じたデザイン コードを発行しました。この規範には、オンライン サービスが従うべき 15 の標準が含まれています (英国情報コミッショナーサービス、2021 年)。ただし、これらは、教育テクノロジープロバイダーが学校を通じて実施する子供向けサービスには適用されません (Digital Futures Commission, 2022)。

南アフリカでは、学校における電子安全に関するガイドラインに監視ソフトウェアに関する規定が含まれており、学習者と教師はオンライン活動が監視されていることを最初に知られる必要があると述べられています。その目的は、アクセスとオンラインでの行動を管理する方法をユーザーに教育し、その行動がプライバシーの合理的な尊重の範囲を超えないようにする、安全なオンライン環境を提供することです。学校の利用規定では、監視ソフトウェアでどのようなデータが取得されるか、データの保存期間、誰がデータにアクセスできるか、権限のないユーザーがデータにアクセスできないようにデータを安全に保管する方法について学習者に知らせる必要があると規定しています。、データが正確であることを保証するためにどのようなメカニズムが存在するのか、そしてデータはどのように使用できるのか (南アフリカ基礎教育省、2017)。

最近の調査では、学習プラットフォームから広告追跡を削除したり（フランス、インドネシア、ブラジルのミナスジェライス州）、学習プラットフォーム（オーストラリアのニューサウスウェールズ州とビクトリア州、エクアドル、スペインの州）に対する調査を開始したりするなど、政府の対応が生じている。カタレーニャ自治州共同体）（ヒューマン・ライツ・ウォッチ、2023）。

ここで説明する規定は、個人情報のオンライン処理に伴うリスクから子どもを守るための一歩前進ですが、権利ではなくリスクに基づいたアプローチに基づいています。

さらに、人権や子どもの権利のデューデリジェンスプロセスと同じ保証は提供されません。監督と監視は、教育テクノロジー企業が標準を遵守し、際限なく権限を拡大しないことを保証する必要があります。苦情の仕組みや行政的または司法的救済は、子ども向けに調整されていない傾向があります。オーストラリア、ブラジル、フランス、アイルランド、シンガポール、南アフリカ、英国は、データ法違反を犯した当事者に対して行政措置を講じる権限を規制当局に委ねています。しかし、調査、民事責任の賦課、罰金の支払いの範囲は国によって異なります。中国の個人情報保護法第 69 条は、個人情報の取扱い者に立証責任を課し、過失がないことを証明できない範囲で責任を負わせます。

ただし、そのメカニズムは複雑であり、そのような主体に責任を負わせるのは依然として難しい可能性があります（教育への権利イニシアチブ、2023）。

プライバシーとデータ保護の侵害の場合、行政罰金は効果的かつ比例的かつ抑止力のあるものでなければなりません。アイスランドでは、監督当局が、米国のクラウドベースの教育会社がレイキャビクの小学校の生徒データを処理する際に保護者の同意を得なかったことがGDPRに違反したとの判決を下し、500万ISK（3万8000米ドル）の罰金を課した（欧州データ保護委員会、2022年）。ノルウェーデータ保護局は、学校職員、保護者、生徒間の通信に使用されるモバイルアプリのセキュリティが不十分だったとして、オスロ市に罰金を課した（欧州データ保護委員会、2019年）。スウェーデンのデータ保護局は、ストックホルムの学校管理のプラットフォームを調査し、セキュリティのレベルが不十分で、児童や生徒を含む「数十万」のデータ主体に影響を及ぼし、機密かつ特別なカテゴリーの個人データを適切に処理していないことを発見した。当局は、

ストックホルム教育委員会に400万スウェーデンクローナ（39万米ドル）の罰金（ストックホルム教育委員会、2020年）。

教育テクノロジー企業は、自社の製品、サービス、システムに健全なプライバシーとデータ保護を適用することで、プライバシーとデータ保護において重要な役割を果たすことができます。場合によっては、これはアプリケーションやデバイスにデフォルトでプライバシーを設定し、ユーザーによる手動入力が必要としないこととなります（ユネスコ、2022）。

Apple のオペレーティング システム iOS 14.5 の場合と同様に、ユーザーはサードパーティ アプリケーションによる追跡をオプトインする必要があります。米国での調査では、アプリによる追跡の許可を与えているユーザーはわずか 13% で、オプトインを求められないように自分で設定しているユーザーは 4% でした（Laziuk、2021）。あるいは、企業は設計によってプライバシーを確保することもできます。GDPR では、満たすべき法的要件として「設計によるデータ保護」が定められています。第 83 条では、この義務の不遵守を処罰対象の犯罪とみなしており、その適切な適用が侵害の重大性を測る基準の 1 つとなっています。

教育テクノロジーのサービスと製品は、その使用から生じるプライバシーと人権への影響を完全に理解できるものにする必要があります。それでもプロバイダーは免除を求めている。オランダでは、政府が Google Workspace for Education のデータ保護影響評価を実施したことを受けて、Google がサービス データに対する契約上のプライバシーに関する取り組みを変更することを提案しました（Bonamigo、2021）。しかし、禁止は解除されなかった（Rao、2022）。オンラインの児童保護が存在する場合でも、設定によっては不連続な場合があります。学校で使用されるサービスやアプリケーションに提供される保護は、子供たちが家で宿題をしている間は必ずしも継続するとは限らず、その結果、子供たちのデータが他のプロバイダーやベンダーによって取得され、その後行動プロファイリングや社会的スコアリングに使用されることとなります（Digital Futures Commission、2022）。

安全上のリスクは無視できない

他の分野と同様に、教育もサイバー攻撃の標的になることが増えています。学校は、社会人口統計から健康記録や財務情報に至るまで、生徒と保護者に関する機密データを保有しています。すべてを守る必要があります。教育システムやユーザーに対する攻撃が増えること、ID やその他の個人データの盗難にさらされる機会が増えることとなります。米国では、45 の学区でサイバー攻撃の影響を受けた学校の数が、2021 年から 2022 年の間にほぼ 2 倍に増加しました（Emsisoft、2023）。世界全体では、2022 年に教育部門がランサムウェア攻撃全体の 5%（APWG、2022）、セキュリティ侵害の 30% 以上を占めました（Verizon、2022）。

“

サイバー犯罪の世界的なコストは、2022年に7兆米ドルと推定されています

”

サイバー犯罪の世界的なコストは、2022年に7兆米ドルと推定されています (Morgan,2022)。身代金が支払われない場合が多いにもかかわらず、学校のサイバーセキュリティが不十分な場合のコストとリスクは大きくなります。これらのコストには、データと作業の損失に加えて、生徒と教師のデータ漏えいの増加、主要なシステムとリソースのダウンタイムと復元が含まれます。米国では、2022年のダウンタイムによる学校や大学のコストは95億米ドル (Bischoff, 2023)、教育におけるデータ侵害の平均コストは2022年に390万米ドル (IBM,2022)と推定されています。43か国の2,700の大学における身代金攻撃の平均コストは約447,000米ドルと推定され (Bluevoyant,2021年)、教育機関が攻撃前の状態を再構築するためにかかる平均コストは、2021年に平均270万米ドルでした。米国では他のセクターよりもはるかに高い (Shier,2021)。教育分野の500人を含む30か国の情報技術意思決定者5,400人を対象とした2021年の調査では、2020年に組織の44%がランサムウェアの被害に遭い、そのうち58%がデータ暗号化の被害に遭ったことが示された。データ暗号化を経験した人の3分の1以上が、平均112,000米ドルの身代金を支払いました。身代金を支払ってもデータの68%しか回復できませんでした (Sophos,2021)。

政府は、デジタルインフラストラクチャとデータをサイバー攻撃から保護するために、適切な法的および政策の枠組みを開発する必要があります。彼らは、テクノロジーの適切な使用と不適切な使用、およびそれらに違反した場合の結果を明確に定義する、強力な許容可能な使用ポリシーを採用できます。サイバーセキュリティのリスクにさらされる機会が増えると、教師、生徒、家族への意識向上と情報提供も必要になります。教育システムを脅威から守るために、防御者のコミュニティと複数の関係者間の協力に基づいた集団防御モデルを確立することは、米国の2021年幼稚園から高校までのサイバーセキュリティ法の重要な要素でした。

ネットいじめに対する安全性と幸福への懸念が高まっている

ネットいじめは、スマートフォンやその他のデバイスへのアクセスによって引き起こされる新しい形式のいじめ行為です。世界では、16%の国が教育に焦点を当てて予防し、それに対処するための法律を制定しています。そのうち38%は、新型コロナウイルス感染症のパンデミック以降にそうしました。について

40%の国がこの分野に関する政策、戦略、計画を持っています。ヨーロッパと北アメリカは、そのような政策を採用している国の割合が最も高い地域 (61%) です (図 8.3)。

ほとんどの国では、ネットいじめとオンライン虐待は他の法律に該当する可能性があるため、明確な犯罪として明確に定義されていません (教育への権利イニシアチブ,2023)。オーストラリアでは、中央、州、準州レベルのさまざまな立法手段により、ストーカー行為、脅迫または脅迫行為、自殺の奨励、名誉毀損、および許可のないオンラインアカウントへのアクセスが犯罪とされています。

2021年オンライン安全法では、ネットいじめの内容を、子供に深刻な屈辱、嫌がらせ、脅迫、または脅迫を与える可能性のあるものと定義し、オンラインサービスプロバイダーに対し、ネットいじめの内容を削除し、経験のある18歳未満のオーストラリア人に対する苦情の管理を要求する権限をeSafety Commissioner局に付与しています。ネットいじめ。2022年個人データ保護法は、インドネシア初の包括的なデータ保護法です。

個人データを扱う公的機関または民間団体にに対し、誤った取り扱いには制裁を加えてデータ保護を徹底するよう求めています。ネットいじめに対する保護は、この法律に基づいて間接的に提供されています。しかし、2008年に改正された電子情報取引法第45B条では、ネットいじめをハラスメントの一形態とみなしています。

日本では「いじめ防止対策推進法」により、オンラインとオフラインの区別なく、国、地方公共団体、学校、教師、保護者のいじめの防止、早期発見・対応の義務が定められている。中国にはネットいじめに関する特別な規定がある。2020年未成年者保護法の第77条および第80条では、「いかなる組織や個人も、未成年者を侮辱、中傷、脅迫したり、悪意を持って未成年者のイメージを傷つけたり、インターネットを通じて未成年者に対してその他のネットいじめ行為を行ったりしてはならない」と規定されています。テキスト、画像、オーディオ、ビデオ。また、ネットワークサービスプロバイダーには、ネットいじめの被害者からの通知を受け取った後、リンクの削除、ブロック、切断などの行為を停止し、情報の拡散を防止するために適時に行動すること、および関連する記録を保管する義務も定めています。ネットいじめを関係当局に報告する (教育への権利イニシアチブ,2023)。

図 8.3: ネットいじめ

を防止し、それに対処するための法律を制定している国は5か国に1つ未満です
教育におけるネットいじめを防止するための措置を講じている国の割合 (ツール別, 2022年)



GEM StatLink: https://bit.ly/GEM2023_fig8_3

出典: Profiles Enhancing Education Reviews (PEER)。

Bangladeshでは、ネットいじめは2006年ICT法(2013年改正)に基づいて処罰の対象となっていますが、教育や学校との明確な関連性はありません。2012～2021年の教育におけるICTマスタープランは、テクノロジーを使用する生徒、教師、管理者の機密性を保護するための特別な措置をサポートしています。2022年データ保護法草案は、データのプライバシーと保護に焦点を当てた国内初の法律です。この法案は教育については触れていないが、児童のオンライン保護全般について言及している。

インドでは、情報技術がネットいじめに対処するための法的根拠と考えられます。この法律は、デジタルおよび情報通信技術を利用して、迷惑で攻撃的かつ侮辱的なコミュニケーションを送信することに対する罰則を規定しています。ネットいじめは、名誉毀損、恐喝、セクハラ、ストーキング、または「女性の謙虚さを侮辱すること」を目的とした言葉、身振り、行為などの犯罪を伴う場合には、刑法に該当する可能性があります。しかし、これらの法律の下では子供には特別な保護は与えられていません。

過度のテクノロジーの使用により、物理的および物理的な損傷が生じます
精神的健康が危険にさらされている

テクノロジーの使用には、デバイスの取り扱いや画面との向き合いに長時間費やす必要があります。教育は特に両方の点で行き過ぎに対して脆弱であり、健康と一般的な幸福に対するリスクを悪化させます。政府はこれらのリスクにどのように対応するかを検討し始めたばかりです。

スクリーンへの曝露は子供の幸福に影響を与える

子どもたちが画面に費やす時間の長さについては、保護者だけでなく教育関係者や医療従事者にとっても懸念が高まっています。米国疾病予防管理センターは、1日のスクリーンタイムを8～10歳で6時間、11～14歳(うちテレビ視聴は5人)で9時間、7.5時間と推定している。15～18歳の場合は時間(CDC, 2018)。

これらのレベルは、新型コロナウイルス感染症のパンデミック中に増加しました。オーストラリア、中国、イタリア、スウェーデン、英国、米国の3歳から8歳の子どもを持つ親2,500人を対象に、パンデミック前後の画面視聴時間を調査したところ、子どもの画面接触時間が1年で50分増加したことが判明した。教育と余暇の両方の結果です。

社会経済的地位の低下は、より大きな増加と関連していた(Ribner et al., 2021)。

国によって違いがありました。ヨーロッパの19か国では、9歳から16歳までの子どもたちが2020年に平均2時間47分をオンラインで過ごしました。スイスの最低2時間14分からノルウェーの最高3時間39分までです。2010年に収集されたデータと比較すると、フランス、イタリア、スペインなどの国ではこの時間が2倍になっています。15～16歳の子供は毎日2時間30分近くをオンラインで過ごしますが、9～11歳では約2時間、12～14歳では3時間12分です(Smahel et al., 2020)。フランスでは、2022年には2歳未満の子供でも毎日3時間11分をスクリーンの前で過ごしました(Le Point, 2023)。

スクリーンタイムに関する懸念は、コンピューターやスクリーンベースのデジタルデバイスが登場するずっと前から議論されていました。しかし、以前の研究の結果は、スクリーンタイムの自己申告のため決定的ではないことが多く、再現エラーやバイアスの影響を受ける可能性がある(Wong et al., 2021)。

最近の研究では、さまざまな分野で悪影響が報告される傾向があります。さまざまな国や地域でのスクリーンタイムに関する89件の研究をレビューしたところ、すべての年齢層でスクリーンタイムの増加が記録されているものの、1日あたりの増加が最も大きかったのは小学生(1時間23分)で、次に大人(58分)であったことが示唆されています。青少年(55分)と5歳未満の子供(35分)。この増加は、食事(例えば、食事の自己規制)、睡眠、精神的健康、目の健康に悪影響を及ぼします(Trott et al., 2022)。

英国では、11歳から16歳の40%が背中や首の痛みを経験しており、親の15%がラップトップ、タブレット、またはコンピューターの使用が原因である可能性が高いとの推定もあります(Sayer Clinics, 2014)。12件の系統的レビューの結果に基づく報告書では、スクリーン時間の増加と不健康な食事、エネルギー摂取量の増加、および肥満のより顕著な指標との間に関連性があることが判明した。1日2時間を超えるスクリーンタイムは、より抑うつ症状、教育成果の低下、睡眠と体力の低下に関連しています。11歳から24歳までの子供と青少年は、1日当たり約2.5時間コンピュータ、3時間電話、2時間をテレビで過ごしていた(Viner et al., 2019)。

米国の2歳から17歳までの若者の大規模なサンプルを分析したところ、スクリーン視聴時間が長いほど幸福度が低下することが示された。好奇心、自制心、感情の安定が低下します。より高い不安;そしてうつ病の診断。これらの関連性の中には、幼児よりも青少年の方が大きかったものもあります(Twenge and Campbell, 2018)。カナダのアルバータ州の母子2,441人を対象とした幼児期の発達に関する研究では、生後24か月と生後36か月の子供のスクリーン時間のレベルが高いほど、それぞれ生後36か月と生後60か月の発達の悪化に関連していることがわかりました(Madigan et al., 2019)。同様の結果が、3歳から5歳の52人の子供を対象とした研究でも報告されており、脳スキャンを使用して各子供のデジタルメディアの使用状況に応じて脳の構造を分析しました。その結果、メディアの使用量が多いほど、皮質の厚さと溝の深さが浅くなることがわかりました。これら2つの特性は、言語発達、読解スキル、複雑な記憶のコード化、共感、顔や感情の表現の理解などの社会的スキルに関連しています(Hutton et al., 2022)。

専門家らは公的介入と上映時間の制限をますます求めている(Nagata et al., 2022)。

6歳から18歳までの25,000人の子どものサンプルを対象とした12のコホート研究と15の横断研究を対象としたメタ分析では、近視のリスクを軽減するために屋外活動を促進する公的介入が必要であると主張した(Duraipandy et al., 2021)。米国カリフォルニア州の学校の2組の6年生を対象とした実験研究では、自然キャンピングに旅行に行き、いかなる種類のデジタル機器の使用も許可されていない生徒の方が、人間の感情を解釈する能力が大幅に優れていることがわかりました。デジタルデバイスに時間を費やし続けた人(Uhls et al., 2014)。



専門家らは公的介入と視聴時間の制限をますます求めている



スクリーンタイムにはリスクがあるにもかかわらず、厳格な規制はほとんどありません。中国教育省は、デジタル機器を教育ツールとして使用するのは全体の授業時間の30%、電子宿題に費やす時間は1日最大20分と制限を設けた。ガイドラインでは、学生が教育的なスクリーンタイムを30~40分間使用した後、10分間目を休める必要があることも示唆しています(Wong et al., 2021)。

政府はゲームにも週最大3時間という厳しい制限を設けており、ゲーム会社にある程度の責任を課している(Soo, 2021)。ゲームでは、すべてのユーザーが実名(Feiner and Kharpal, 2021)と政府発行の身分証明書(Zhang, 2021)を使用して登録する必要があります。

韓国では最近まで、15歳までの子供が夜間にビデオゲームをすることは禁止されており、この規定は2011年青少年保護改正法に定められていたが、この規定は2021年に廃止された。ミネソタ州は2022年に、公立の幼稚園と幼稚園の生徒が教師の関与なしに一人でスクリーンを使用することはできないと定める法律を可決しました(ミネソタ州教育省, 2021)。

ガイドラインや推奨される視聴時間の制限は、ほとんどの場合保健当局の管轄下にあります。それに従うかどうかは親の責任です。身体活動、座りっぱなしの行動、睡眠に関する世界保健機関のガイドラインでは、1歳から5歳までの子どもの座りっぱなしの画面視聴時間は1時間未満であることが推奨されています(WHO, 2019)。オーストラリアでは、子どものための24時間行動ガイドラインが次のことを推奨しています。2歳未満の子どもにはスクリーンタイムを禁止します。1時間以内

2歳から5歳の場合は1日あたり。5歳から17歳の場合、座って娯楽としてスクリーンに映る時間は1日あたり2時間以内です(学校の勉強は含まれません)。しかし、これらのガイドラインを満たしているのは未就学児の17%~23%、5~12歳児の15%のみでした(Joshi and Hinkley, 2021)。

一部の国は厳しい制限を課すのではなく交渉を推奨している。カナダでは、カナダ小児科協会のガイドラインは、親と子供にとって大きなストレス源となる可能性があるスクリーンの使用時間制限から遠ざかるために、スクリーンの最小化、緩和、注意深い使用、および健康的な使用のモデル化という4つの原則を強調しています(Ponti, 2022)。同様のアプローチは英国でも見られ、英国王立小児科小児保健大学は、親が対話を通じて子供のスクリーンタイムを管理できるようにするためのガイドラインを発行しました(Viner et al., 2019)。2020年、ルクセンブルク国民教育・児童・青少年省とBEE SECUREイニシアチブは、合理的なスクリーンの使用についての親の認識を促進するために、「Screens in the Family」というキャンペーンを立ち上げました(ルクセンブルク国民教育・児童・青少年省、2020;ルクセンブルク国民教育省児童青少年およびBEESECURE、2022)。

いくつかの国では学校での電話やその他のテクノロジーを禁止しています

データのプライバシー、安全性、幸福に対する懸念も、学校、特に若い年齢の生徒による一部のテクノロジーの使用に関する議論の根拠にあります。学校でのスマートフォンの使用には議論の余地がある。ベルギー(Baert et al., 2020)、スペイン(Beneito and Vicente-Chirivella, 2020)、イギリス(Beland and Murphy, 2016)の研究では、学校からの携帯電話の使用を禁止すると、特に成績の悪い生徒の学業成績が向上することが示されています。

この報告書の分析によると、世界ではほぼ4か国に1か国がそのような禁止を法律または政策で導入していることが示されています。特に、13%の国には携帯電話を禁止する法律があり、14%には携帯電話を禁止する政策があります。禁止は中央アジアおよび南アジアでより一般的です(図8.4)。2011年、バングラデシュは教室内の教師による携帯電話の使用を禁止しました(Samad, 2011)。2017年、学校や大学の学生と教師の両方が教室に携帯電話を持ち込むことが禁止されました(bdnews24, 2017)。

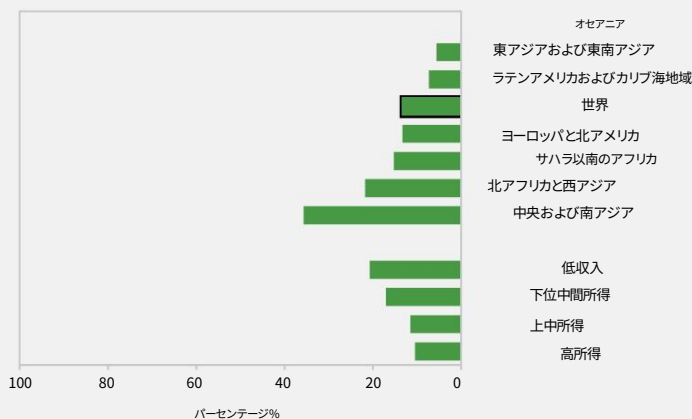
タジキスタンの教育法第25条では、初等学校、職業学校、中等学校における生徒による携帯電話の使用が禁止されています。ウズベキスタンでは、学校に入るときにすべての機器の電源を切ることが法律で義務付けられています。

図 8.4: 7 か国に

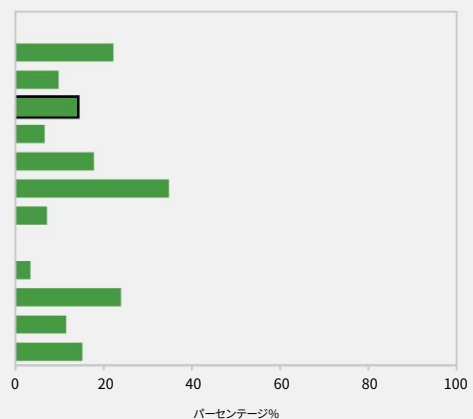
1 か国が学校での携帯電話の使用を法律で禁止しています

学校での携帯電話使用を禁止する措置を講じている国の割合 (ツール別、2022 年)

a. 法



b. 方針、計画、戦略、またはガイドライン



GEM StatLink: https://bit.ly/GEM2023_fig8_4

出典: Profiles Enhancing Education Reviews (PEER)。

オーストラリアのニューサウスウェールズ州教育省は、2018年に公立小学校でのモバイル機器の使用制限を実施しました（ニューサウスウェールズ州政府、2020年）一方、タスマニアではすべての公立学校の生徒に携帯電話の使用が禁止されています（タスマニア政府省教育とトレーニング、2019年）およびビクトリア（Gullaci、2019年）。しかし、オーストラリアの1,070人を対象とした世論調査では、回答者の3人に2人が、学校でのすべての生徒の携帯電話の使用を禁止するのではなく、生徒に携帯電話の安全な使用方法を教育するデジタル安全プログラムの導入を強くまたはある程度支持していることが判明した。半数以上が全生徒に対する携帯電話の使用禁止を支持またはある程度支持している一方、37%は学校内での携帯電話の使用を11年生と12年生のみに支持またはある程度支持している（Essential Research、2022年）。

フランスでは禁止令があるが、特定の学生グループ（障害者など）やスマートフォンが「教育」目的で使用される場合は例外としている（フランス国民教育省、2018年）。ラトビア、メキシコ、ポルトガル、スペイン、スイス、米国に加え、オントリオ（カナダ）とスコットランド（英国）でも全面的または部分的な禁止が課されている。しかし、大韓民国では監視機関が、完全な禁止はコミュニケーションの自由などの学生の基本的権利を侵害すると主張した（Hyo-jyn、2021）。

“

学校でテクノロジーとそれに伴うリスクを扱うには、禁止以上の何かが必要になるかもしれない

”

ブルキナファソでは、2018年の命令により、中等学校内での携帯電話と付属品の使用は没収の罰則のもとで禁止されており、機器は年度末まで生徒に返却されずに保管されることになっている。

コースまたは評価で許可されている以外のデバイスの使用は禁止されており、違反を繰り返した場合、学生は一時的または永久的に除外されます。コートジボワールでは、省令で学校内での携帯電話の使用が禁止されており、2018年の命令では試験中のデジタル通信メディアの使用が禁止されている。ギニアでは2021年の決定で、学校内でのスマートフォンやその他のインターネットに接続されたデバイスの使用が禁止された。

各国は、アプリケーションの動作に不必要なユーザーデータを収集する際にプライバシー上の懸念が生じるため、教育現場での特定のアプリケーションの使用を禁止しています。デンマークでは、Google Workspace for Education と Chromebook に関してヘルシンゲル市が実施したデータ保護影響評価により、学校での使用が禁止されました（Schmiedt、2022）。フランス教育青少年省は、学校での Microsoft Office 365 と Google Workspace の無料版の使用を禁止しました（UC Today、2022）。ドイツでは、Microsoft 製品は GDPR に準拠していないため、バーデン ヴュルテンベルク州とヘッセン州で禁止されています（Schneider、2022）。オランダのデータ保護当局は、児童のデータ保護とプライバシーに関する規制違反を理由に、Chromebook と Google Workspace for Education の学校への使用を 2023 年 8 月まで禁止することを提案しました（Toulas、2022）。

米国のいくつかの学校や大学も、TikTokやその他のプラットフォームの禁止を開始している（Ksetri、2023）。2023年3月に発行された大統領令は、国の「安全保障、経済、民主主義」に対するテクノロジーの重要性を強調すると同時に、「テクノロジーが普遍的な人権に従って開発、導入、統治されること」を保証するとしている。法の規則;そして適切な法的認可、保護措置、および監督」（米国大統領、2023年）。

テクノロジーの統合によって学習が改善されない場合、または生徒の幸福度が悪化する場合には、学校でのテクノロジーの禁止は正当である可能性があります。しかし、学校でテクノロジーとそれに伴うリスクを扱うには、禁止以上の何かが必要になるかもしれません。まず、学校で何が許可され、何が禁止されているかをポリシーで明確にする必要があります。学生に求められる行動が明確または透明性がない場合、学生を罰することはできません。これらの分野での決定には、確かな証拠に裏付けられた対話が必要であり、生徒の学習に関係するすべての人々が参加します。第二に、これらの新しいテクノロジーが学習において果たす役割と、学校内および学校内での責任ある使用について明確にする必要があります。第三に、学生はテクノロジーに伴うリスクと機会を学び、重要なスキルを開発し、テクノロジーの有無にかかわらず生活することを理解する必要があります。

新しい革新的なテクノロジーから学生を守ることは、学生を不利な立場に置く可能性があります。将来を見据えてこれらの問題を検討し、世界の変化に合わせて調整し適応する準備をしておくことが重要です。

結論

テクノロジーは、子どもたちが教育とプライバシーの両方に対する権利を含め、権利を行使し実現する方法を根本的に変えました。特定の条件下では、教育におけるテクノロジーの使用は子どもたちの学習の機会を高めることができますが、子どもたちの身体的および精神的な完全性、プライバシー、尊厳を危険にさらす可能性もあります。

知的財産、データプライバシー、オンラインの安全性に関連する問題は、各国が対処する必要がある重要な課題です。

デジタル教育戦略に加えて、多くの国、主に高所得国は、GDPR に基づいてデータ保護法または規制を発行しました。しかし、個人データの取り扱いに関して、大人と子供を区別していないことがよくあります。子どもたちは特別な保護を受ける権利があるため、子どものデータ保護法と基準、および子どもに合わせた説明責任の仕組みがますます必要とされています。政策立案者は、オンライン活動中に子どもたちの権利が保護されるよう、子どもたちの声に耳を傾けるべきです。

健全な教育テクノロジーとデータガバナンスは、テクノロジーの恩恵をより公平で質の高いものにすると同時に、学校が子供たちにとって学び、遊び、発達し、成長するための安全な場所であることを保証するために不可欠です。この目的を達成するには、明確な枠組み、効果的な規制、監視、紛争解決メカニズムを設定する必要があります。

何十億もの人々が接続され、学習中にデータや情報を交換する世界では、教育を受ける権利とプライバシーの権利を監視し、保護する必要があります。