

5.3

Estonia's education system in the winds of technological and legal change

Kaido Kikkas and Riin Saadjärv

KEY MESSAGES

- Estonia's education sector has sought to keep pace with technological and legal change, though with mixed success.
- New technological solutions – especially artificial intelligence – require appropriate regulation, along with broader consideration of their impact. Every major technological advance brings new security and privacy risks, and the entire digital technology market needs regulation through quality standards.
- The current alignment with the interests of large corporations must change – vendor lock-in poses a problem in the long term.
- The focus should be on learners' needs rather than on technological possibilities.

INTRODUCTION

Technology evolves rapidly while the law is inherently stable. When a slowly changing legal framework must regulate fast-developing technology, problems arise. This issue has been discussed for years – for example, it was addressed by the World Economic Forum in 2018¹ – and the debate has only intensified since the Covid-19 pandemic and the subsequent boom in AI.

Since the days of the Tiger Leap (Tiigrihüpe) programme, Estonia's education system has consistently sought to keep pace with new trends. At the turn of the century, e-learning and, with it, the open educational resources movement reached Estonia. Meanwhile, progress has long been hindered by the dominance of a few large corporations whose products control key

technological tools and environments, leading to the problem of vendor lock-in. Moreover, every significant technological advance has brought with it new risks to security and privacy.

NEW DEVELOPMENTS, NEW PROBLEMS: SECURITY AND PRIVACY

As noted earlier, nearly every technological innovation brings new risks. In Estonia's education landscape, a wide range of security issues has already emerged – from long-standing concerns such as weak password practices and online scams to newer challenges like deepfakes and data privacy in AI training. The main areas of concern in this field can be summarised as follows:

- **Cyber threats.** The education sector is targeted much like businesses and government agencies, and the range of attackers and motives is broad – from a mischievous student's prank to the actions of organised groups seeking to steal, alter or destroy data. Examples include the cyberattack on Tartu Health Care College on 4 September 2020² and the ransomware attacks in 2024 targeting Järvamaa Vocational Training Centre and Tallinn Health Care College.³
- **Device-related risks.** Smart devices are widely permitted across Estonia's education sector, and the line between institutional and personal devices is often blurred – for example, in terms of network access. Risks therefore arise both from insufficiently regulated device use (including smartphone dependency) and from poorly managed bring-your-own-device (BYOD) policies, such as inconsistent software versions and missing security updates across devices.
- **Physical environment risks.** In addition to classic network-based cyberattacks, educational institutions must also address threats that exploit physical infrastructure.
- **Insider threats.** For example, on 5 November 2020, a schoolboy from Rapla ordered a cyberattack against his own school.⁴

- **Data protection.** In education, this includes safeguarding data about students and staff, as well as managing access rights for parents and other authorised parties. In one case in 2021, a parent petitioned the Chancellor of Justice to restrict another parent's access to their child's e-school account.⁵
- **Data handling by external services.** Schools today rely on a wide range of external digital services – from web-based learning applications, learning management and information systems to cloud platforms, social media and, increasingly, AI applications. It should be noted that almost all well-known large language models (LLMs) operate as cloud services, meaning that user queries are stored on remote servers outside the user's direct control.

When shaping the legal framework, a good starting point would be for each educational institution to establish or update its information security policy. As noted in the Estonian Information System Authority's (RIA) cybersecurity yearbook,⁶ one way to mitigate risks is to apply the Estonian Information Security Standard (E-ITS) within the education sector.⁷

OFF-THE-SHELF SOLUTIONS: CONVENIENT BUT RISKY FOR SCHOOLS

Debates about the role of digital technologies in education have expanded in recent years – from post-pandemic digital fatigue to the need to limit the use of smart devices and the transition to e-examinations. Since the national curriculum⁸ places digital competence at the core of education, it is essential that achieving this competence does not depend on a student's place of residence, school type or family's socioeconomic status.

In Estonia, responsibility for covering school expenses and procuring IT equipment lies with the school's governing body – for general education schools, this is usually the local government.⁹ However, local governments' capacity to invest in technology varies considerably, depending primarily on their economic resources but



also on their priorities. As school owners, local governments have the right to establish general rules for school operations, including the use of digital tools and technologies, but schools typically retain the freedom to choose solutions not centrally procured by the municipality.

All schools within the same local authority typically rely on either Microsoft or Google for Education as their core services. A survey conducted among school educational technologists in summer 2024 found that 62% of respondents worked in schools using Google for Education.¹⁰ By contrast, state upper secondary schools have moved towards unified use of the Microsoft 365 cloud service to simplify coordination. Using a single cloud service is not inherently problematic if it meets the school's needs and reduces administrative workload. However, it is important to bear in mind that service providers' terms and conditions often make switching providers difficult, and when a school or local authority wishes to change due to evolving expectations, this may not be easy to implement. Even when relying on a single provider, teaching digital competence should prioritise functions and transferable skills rather than the ability to use specific applications – for example, learning to create presentations to express ideas rather than to use PowerPoint in particular. This helps ensure that learners are prepared, at the next stage of education or in the labour market, to work with tools offered by different providers.

EDUCATIONAL TECHNOLOGY IS NOT A TEACHER

The intelligent use of educational technologies can diversify the learning process and support the development of students' digital competence. However, since Estonia has not established common rules for the use of educational technologies, practices vary. The latest PISA study¹¹ showed that 47.5% of Estonian students use computers for learning at least once a week, spending an average of 1.6 hours per day on this activity – 0.3 points below the international average. Estonia has thus lost its leading position in the use of digital technologies in schools. This raises the question of whether this situation results from school autonomy (depending on school leadership and teachers' readiness and

awareness of meaningful technology use), from the market-based logic of educational technology provision (depending on the resources of school owners), or from something else entirely – for example, decisions in other countries to make substantially greater investments in schools' technological capacity.

The absence of uniform quality standards, limited resources and constrained procurement options have all hindered the widespread adoption of educational technology solutions in Estonian schools. At present, schools must ensure that all learning tools – including digital technologies – comply with relevant legislation, such as the General Data Protection Regulation (GDPR) and the Estonian Copyright Act.¹² The Ministry of Education and Research and the Education and Youth Board (Harno) provide recommendations for the purposeful use of educational technology¹³ and also organise related training.¹⁴ However, adherence to these guidelines is not mandatory. Schools may also specify in their curricula and internal rules the principles, aims and conditions for using digital tools and applications, and many publicly list the environments they use and their purposes to keep all stakeholders – including parents – informed. It is crucial that no school-level rules contradict national laws or agreements.

Ultimately, it must be emphasised that no educational technology improves learning outcomes on its own, and passive technology use may even have a negative effect. Much greater attention should be given to how digital tools can enrich the learning process.¹⁵ Going forward, teachers should be supported through common quality standards that enable them to assess how well available solutions align with contemporary learning approaches and support the achievement of learning outcomes – and how different educational technologies can be integrated effectively within the learning process.

OPEN EDUCATIONAL RESOURCES REMAIN ESSENTIAL

For example, Hans Põldoja¹⁶ has repeatedly addressed the issue of open educational resources, and several relevant articles appeared in the once-popular E-Learning Newsletter,¹⁷ which

ceased publication in 2016. For a long time, the main issue stemmed from the tension between rigid interpretations reflecting the positions of the World Intellectual Property Organization (for example, in the autor.ee portal) and the everyday realities of schools. Limited resources, coupled with the perceived complexity of the topic, led in practice to resignation and indifference.

A significant milestone came in 2010 with the official Estonian translation of the Creative Commons core licences (version 3.0), which helped bring this licensing model – highly suitable for education – into broader public awareness. Several open-licence learning environments emerged at the time (VIKO, IVA, LeMill and others, while some enthusiasts also contributed under the Wikipedia-related Wikiversity project), and some of these developed strong communities of content creators. In 2016, the Estonian Ministry of Education and Research launched the e-Schoolbag (e-Koolikott) project, based on the Estonian version of the CC BY-SA 3.0 licence.¹⁸ The Covid-19 pandemic gave the field fresh momentum by forcing schools to adopt e-learning and digital tools, which in turn required corresponding legal frameworks – guidelines were subsequently issued by both the Ministry of Education and Research¹⁹ and the Education and Youth Board.²⁰

On the one hand, the current situation seems to have returned to where it was at the beginning of the century, with copyright issues recently overshadowed by seemingly more pressing topics. On the other hand, the rise of cloud services and AI applications – especially those based on large language models, such as ChatGPT – has brought a new wave of challenges to educational web content, including questions of authorship for AI-generated material. Vendor lock-in imposed by major corporations remains a persistent problem. In addition, beyond copyright, another key piece of European legislation shaping education is the General Data Protection Regulation (GDPR). In the near future, the EU Artificial Intelligence Act, which entered into force on 2 August 2024 and will be fully applicable from August 2027, will further influence the legal landscape.²¹

From a copyright perspective, the greatest challenge today lies in adapting and differentiating learning materials, both of which require

modifying existing content. Teachers therefore need to understand the conditions attached to different licences and should be more actively encouraged to use existing resources – such as those in the e-Schoolbag environment – that allow modification where necessary.²²

Much has been said about AI's potential to optimise learning design, management and feedback. While AI can certainly support teachers' work, it is essential to have a clear understanding of which actions are permitted and which are not in terms of data handling. It must also be emphasised that responsibility for the lawful processing of data always lies with the person handling the data, not with the platform itself.

For this reason, continued attention to this field is crucial, including (a) integrating new technologies into the legal framework, (b) providing ongoing training and awareness-raising to ensure sustainable content creation, and (c) preventing vendor lock-in in education.

VENDOR LOCK-IN – EASILY CAUGHT IN, HARD TO ESCAPE FROM

Vendor lock-in, as defined by the TechTarget portal, is 'a situation in which a customer using a product or service cannot easily transition to a competitor's product or service'.²³ To this definition, one might add: 'as a result of the provider's deliberate actions'.

The most extreme form is monopolistic lock-in, where a single player dominates the market and all users are forced to accept this reality. Breaking such a monopoly from below is difficult, if not impossible – it typically requires state intervention.²⁴ While such cases are rare in Estonia's education system, monopolies are not the only path to dependency. Another significant form is non-monopolistic collective lock-in, whereby a sufficiently large number of users adopt a product or service, making alternative options directly or indirectly too costly to pursue.

Lock-in also occurs at the individual level; this is the softest form of dependency, where users' preferences and habits blend with subtle



persuasion ('I've driven a Ford all my life – why change now?'). Though not serious in isolated cases, this form of lock-in can easily spread: for example, when a company's new manager decrees that everyone must use a particular brand of phone, individual dependency becomes institutional.

There are also forms of lock-in that appear easy to escape but carry undesirable side effects. This will be familiar to anyone who has tried to quit a major social media platform. Even if the account can be deleted, doing so may sever real-world connections, especially with contacts abroad.

Many large corporations whose services have long been used in higher education have employed lock-in strategies to maintain or expand their market share. Microsoft has decades of experience monopolising file formats (the best-known example being the long-running struggle over MS Office formats), Google has been successful in achieving collective lock-in through its cloud services, and Apple fully controls both its hardware and software ecosystems. While this is advantageous for the company, the risks fall largely on users.

Substantial price discounts on proprietary software – so-called academic licences – serve as another tool for achieving collective lock-in. Every educational institution that uncritically commits itself to a single platform contributes to the emergence of a wider software monoculture across society. Yet with goodwill and determination, lock-in can be resisted even in universities. For example, the University of Pretoria in South Africa successfully replaced its long-standing, costly dependency on AutoCAD with a free and open-source alternative.²⁵

Why is vendor lock-in a problem? The most immediate concern is economic: under normal conditions, prices are regulated by the balance of supply and demand. When a provider achieves a monopolistic position through lock-in, it can dictate prices and choose which clients to serve and how. For example, Microsoft Office lacked an Estonian-language version for many years, and it was introduced only after a sufficiently strong alternative – the then-popular OpenOffice.org – had emerged.

Beyond economics, lock-in poses risks for security, privacy and data protection. A situation in which all computers in an organisation use identical software – as is often the case with vendor lock-in – creates what is known, borrowing from biology, as monoculture, a condition whose associated vulnerabilities have long been recognised.²⁶ A recent example in Estonia illustrates this point: the country's relatively heavy reliance on Microsoft software magnified the global service disruptions caused by an error at one of Microsoft's partner firms. The consequences were far more severe than they would have been in a more diversified technological environment.

Avoiding lock-in from the bottom up requires conscious choices, accountability, determination and collaboration among users – and, by default, the absence of corrupt influence. Occasionally, lock-in may ease naturally due to technological advancements. A well-known example is the standardisation of power cables for cameras and smart devices: while each major brand once had its own proprietary connector, USB has now become the de facto standard. However, such organic resolutions cannot always be relied upon.

Estonia – including its education sector – must therefore pay much closer attention to vendor lock-in and how to prevent it. Decision-makers should eliminate the temptation to delegate responsibility to external providers ('Let Google handle it') and instead make greater use of domestic services, which would also benefit the national economy. A practical first step would be to reduce existing lock-in by identifying and implementing alternatives – for example, ensuring that Microsoft-based cloud services function smoothly across other operating systems.

Where is this trend heading? AI is rapidly gaining ground in Estonia's education system. The services that make this possible – ChatGPT and others – are, technically speaking, cloud-based services similar to solutions previously offered by providers such as Google and Microsoft. The issues of lock-in and choice are likewise similar. Once again, Estonian education faces a decision between the apparently easier path of outsourcing responsibility to global tech giants – becoming a small client with little influence – and the more demanding but ultimately more sustainable role

of self-reliant owner. Just as Estonia needs an Estonian-language Wikipedia and well-localised software, its linguistic and cultural sphere also needs cloud services and AI solutions that reflect local contexts and support the Estonian language – without becoming overly dependent on a single major provider. A good example is the debate that unfolded in early 2025 over making the Estonian language corpus available to Meta for training its AI models.²⁷

SUMMARY: ESTONIA MUST ONCE AGAIN ADAPT TO CHANGE

As of 2026, Estonia's education system is reaching a point where many long-standing practices and mechanisms need to be reassessed. The e-learning solutions adopted out of necessity during the Covid-19 pandemic were followed by new priorities in information and communication technology (ICT) – such as introducing flexible hybrid learning alongside traditional in-person and online teaching – and later by shifts driven by advances in AI. Technology has once again accelerated, and the legal system must be able to keep pace.

ICT development in Estonia's general education schools is largely fragmented and depends heavily on the financial capacity of local governments, the knowledge and priorities of school leadership, and their willingness to allocate limited resources to technological development. Moreover, there is often no overarching vision, and the technologies in use are viewed as isolated components rather than parts of an integrated whole. One seemingly convenient 'lifeline' has been the outsourcing of technological responsibility – for example, by adopting the solutions of a single provider across the board.

Schools should begin by focusing on the pedagogical needs of teaching and learning, and only then identify the technological solutions that best support those needs. This requires an approach in which ICT infrastructure, both paid and open-source software, digital learning environments and educational materials form a purposefully designed and coherent system.

If the current situation persists – where the renewal of technology and access to educational tools depend largely on the financial capacity of school owners and the attitudes of school leaders – disparities in access to modern learning environments and contemporary teaching and learning opportunities will continue to grow. These differences could be reduced through a nationally coordinated approach that is both open and legally grounded. The state-provided e-Schoolbag platform, with its Creative Commons licensing model, serves as a good example of such a framework.

REFLECTION

Margus Pedaste

Vendor lock-in is widespread in Estonia's education system and poses a serious threat to the smart development and use of digital solutions. At the University of Tartu, Microsoft products dominate; at Tallinn University, Google services; in schools, either Google for Education or Microsoft 365 are prevalent, alongside devices and applications from various Asian manufacturers. Learning management systems also vary – Moodle, eKool and Stuudium, among others. Once a particular system is adopted, integrating tools from other providers often becomes difficult. In some cases, these barriers are deliberately created by vendors; in others, they stem from our own limited capacity to ensure universal access and support, compounded by habit.

Every digital tool or device carries potential risks for users – from cyberthreats to dangers related to device use and data processing. If we wanted to be truly secure in the digital realm, the only logical step would be to stop using digital solutions altogether. But is that what we want? How great is the benefit of digital innovation, and when does it justify taking certain risks? How can we mitigate those risks and ensure the resilience of the digital ecosystem? In teachers' professional standards, resilience is defined as the ability to cope with change on emotional, cognitive and behavioural levels, responding appropriately and restoring balance for self-care. How well can we manage when a digital product or service disappears, or when a new one appears? Can we prioritise our learning or teaching goals and, when necessary, adjust our behaviour quickly and thoughtfully – one might say organically – to incorporate different digital possibilities into the process?

What would it take to allow digital innovation to thrive?

The national system must support flexible integration between different technology providers. If the goal is to use the best solutions and focus on learning outcomes rather than mastering a specific tool, schools must not be

divided between 'Microsoft schools' and 'Google schools' or similar. When technology giants show little interest in interoperability, we should consider how to support it at the national level to reduce the risk of educational inequality. It would help if new solutions were procured centrally for all schools, while each institution remains responsible for supporting teachers and learners in their use.

Teachers require strong digital competence. A teacher is both a guide for learners and a continual learner themselves. A learning professional does not shy away from new challenges or cling to old habits but faces them head-on, explores, experiments and, when results are positive, adapts existing practices. At present, teachers' digital competence is not assessed in Estonia, yet OECD PISA data show that the use of digital tools for learning correlates more strongly with lower mathematics performance here than in most other countries. This indicates that teachers' digital competence is alarmingly low and in urgent need of systematic development. Those without digital skills cannot take advantage of digital opportunities, and in this way, we waste our potential.

We must reduce fears surrounding copyright, data protection and artificial intelligence. In education, there has long been a sense that much of the available digital content cannot be used legally because of copyright restrictions and cost, coupled with limited resources. While copyright is indeed important, studies on the educational exception conducted at the University of Tartu a few years ago revealed that the situation is far less restrictive than often assumed. The educational exception allows for extensive use of materials for learning within a closed environment. Meanwhile, new anxieties have emerged around data collection, data use and AI hallucinations. Striking a balance requires raising public awareness, which is the foundation for the confident and intelligent use of digital solutions.



REFERENCES

1. D. Malan, The law can't keep up with new tech. Here's how to close the gap. – Emerging Technologies, World Economic Forum, 21.06.2018.
2. L. Karu, Tervishoiukõrgkooli tabanud küberrünnak löi serverid sassi. – *Tartu Postimees*, 15.09.2020.
3. Cyber security in Estonia: Estonian schools should prioritise cybersecurity. – Estonian Information System Authority, 2025, <https://www.ria.ee/en/estonian-schools-should-prioritise-cybersecurity>.
4. S. Jõgis, IT-spetsialist: Ei ole üllatav, et koolinoor oskas tellida küberrünnaku. – *Raplamaa Sõnumid*, 20.04.2021.
5. Ü. Madise, Õiguskantsleri aastaülevaade 2021/22: Lapsed ja noored (Õiguskantsleri büroo, 2022).
6. Cyber security in Estonia: Estonian schools should prioritise cybersecurity. – Estonian Information System Authority, 2025, <https://www.ria.ee/en/estonian-schools-should-prioritise-cybersecurity>.
7. See also <https://digiriigiakadeemia.ee>.
8. Põhikooli riiklik õppekava [National curriculum for basic schools]. – *Riigi Teataja* I, 29.08.2014, 20.
9. Riigieelarve seaduses kohaliku omavalitsuse üksustele määratud toetusfondi vahendite jaotamise ja kasutamise tingimused ja kord [Conditions and procedure for the allocation and use of support fund resources assigned to local authorities under the State Budget Act]. – *Riigi Teataja* I, 30.01.2018, 19.
10. Eesti haridustehnoloogide ülevaade kasutatavatest operatsioonisüsteemidest, rakendustest, keskkondadest üldhariduskoolides [Overview by Estonian educational technologists of operating systems, applications and environments used in general education schools]. Study conducted by the authors, 2024.
11. G. Tire (ed.), *PISA 2022. Eesti tulemused* (Haridus- ja Noorteamet, 2023).
12. Põhikooli- ja gümnaasiumiseadus [Basic Schools and Upper Secondary Schools Act]. – *Riigi Teataja* I, 21.03.2015, 16.
13. Üldised põhimõtted teoste kasutamisel haridusasutustes. – Haridus- ja Teadusministeerium, last updated 1.11.2022, <https://hm.ee/uldised-pohimotted-teoste-kasutamisel-haridusasutustes>.
14. Distsantsilt targemaks veebiseminarid. – Haridus- ja Noorteamet, last updated 1.10.2025, <https://harno.ee/distsantsilt-targemaks-veebiseminarid>.
15. Digiefekt: Projekti tutvustus. – Tartu Ülikool, 2023, <https://digiefekt.ut.ee/projekti-tutvustus>.
16. H. Põldoja, Õppematerjalid ja autoriõigus. Presentation at Tallinn Lilleküla Secondary School, 2007.
17. <https://uudiskiri.e-ope.ee/>
18. <https://e-koolikott.ee/>
19. M. Varma, Teose autoriõigusi tuleb järgida ka koolikeskkonnas. – Haridus- ja Teadusministeerium, 14.11.2022, <https://www.hm.ee/uudised/teose-autorioigusi-tuleb-jargida-ka-koolikeskkonnas>.
20. Mida peaks õpetaja teadma intellektuaalomandist ja autoriõigustest? – Blog, Haridus- ja Noorteamet, 26.04.2022.
21. See also Artificial Intelligence Act. – Council of the European Union, last updated 29.04.2025, <https://www.consilium.europa.eu/en/policies/artificial-intelligence-act/>.
22. <https://e-koolikott.ee/>
23. K. T. Hanna, Vendor lock-in. – TechTarget, 19.05.2023, <https://www.techtarget.com/searchdatacenter/definition/vendor-lock-in>.
24. M. Stamp, Risks of monoculture. – *Communications of the ACM* 47 (3), 2004.
25. B. Collette, R. Dodd, Autodesk is teaching students hard life-lessons about vendor lock-in. – Ondsels, 20.10.2023.
26. M. Stamp, Risks of monoculture. – *Communications of the ACM* 47 (3), 2004.
27. M. Juha, Kas Eesti peaks Metale andma eesti keele korpuse? – ERR, 21.02.2025.