Gewerkschaft
Erziehung und Wissenschaft
AG Digitalisierung
Bezirk Köln

Digitales Arbeiten in der Schule – ein Dilemma

Die Corona-Krise hat uns allen eines gezeigt: Die Schulen in Deutschland sind auf virtuelles Lernen, z.B. in Lernclouds oder mit Videokonferenzsystemen, denkbar schlecht vorbereitet. Jede Schule und teilweise sogar einzelne Lehrkräfte versuchen auf sich selbst gestellt schnelle Lösungen zu finden. »Office 365« (in der Privatversion nun »Microsoft 365«) und/oder als Teil davon »Microsoft Teams«[1] wird von vielen Schulträgern, Schulleitungen, Kolleg*innen, aber auch von vielen Eltern favorisiert und manchmal sogar eingefordert. In der Tat bietet dieses System viele Möglichkeiten und ist komfortabel zu bedienen, es gibt aber auch gravierende Bedenken hinsichtlich des Datenschutzes[2].

Viele Lehrkräfte fühlen sich zu Recht überfordert, auch weil das MSB bislang nur unzureichend eigene Lösungen anbietet und klare Aussagen zur Zulässigkeit von kommerziellen Lösungen scheut. Da die Verantwortung für Entscheidungen zum digitalen Lernen daher bei den einzelnen Schulen bzw. Lehrkräften liegt, möchten wir informieren und dazu anregen, sich mit digitalen Diensten und Plattformen kritisch auseinanderzusetzen.

Warum überhaupt Datenschutz?

Dienste wie Office 365/Teams, aber auch viele weitere in der Schule genutzte Dienste sammeln Verhaltensdaten ihrer Nutzer*innen, sie analysieren die anfallenden Daten automatisiert und nutzen sie für verschiedene Zwecke (auch in Fällen, in denen die Schüler*innen keinen Account anlegen). In wenigen Fällen gibt es spezielle Schulversionen, für die Datensparsamkeit wenigstens versprochen wird. Auch wenn Unternehmen (wie jüngst Microsoft für Teams[3]) behaupten, Nutzer*innendaten nicht für Werbung zu verwenden, sollte man dies kritisch hinterfragen, da weitere, jetzt und in Zukunft mögliche, Nutzungen persönlicher Daten in diesen Statements bewusst nicht erwähnt werden. Solche Aussagen werfen eher die Frage auf, ob Nutzer*innen nicht bewusst in die Irre geführt und aufkeimende kritische Gedanken beruhigt werden sollen.

Natürlich wollen Mitarbeiter*innen dieser Dienste nicht eine hochgeladene Gedichtsanalyse unserer Schüler*innen lesen, aber sehr wohl besteht ein Interesse an der Auswertung von Metadaten wie der Textlänge, der durchschnittlichen Wortlänge, der Anzahl der Rechtschreibfehler (Erkenntnisse über Schreibkompetenzen) oder der Anzahl der Uploads. Generell interessieren sie alle Daten, die Rückschlüsse über das Arbeitsverhalten der Nutzer*innen zulassen. Mit diesen Metadaten können von den Nutzer*innen Persönlichkeitsprofile erstellt werden.

Wofür diese Erkenntnisse jetzt und in Zukunft verwendet werden, kann nicht sicher vorhergesagt werden. Zum Beispiel könnten sie mittelfristig in die Herstellung von Künstliche-Intelligenz-Systemen zur Vorhersage von Leistungsfähigkeiten von Nutzer*innen einfließen. Technisch machbar wäre auch eine Art »Schufa-Auskunft«, bei der Arbeitgeber Ratings zu Bewerber*innen abfragen: »Wie war das bisherige Arbeitsverhalten? Rät mir die Statistik zur Einstellung oder nicht?«

Auf einen Teil der Daten haben schon jetzt auch die Administrator*innen an der eigenen Schule Zugriff. Damit erhalten sie teilweise tiefgehende Einblicke in das Arbeitsverhalten von Kolleg*innen und Schüler*innen.

Für das Unternehmen Google, das auch im Bildungsbereich aktiv ist, ist das Verkaufen von Persönlichkeitsprofilen vor allem in Zusammenhang mit Werbung schon jetzt das hauptsächliche Geschäftsmodell. Für andere Anbieter (Apple, Microsoft, u.a.) muss man zumindest die Befürchtung hegen, dass dies in Zukunft geschehen könnte. Wenn unüberlegte Instagram-Postings in einem Bewerbungsgespräch zu Nachteilen führen, ist das ärgerlich, liegt aber letztlich in der Verantwortung der Bewerber*innen selbst. Wenn im Schulbereich angefallene Daten später an unerwarteter Stelle wieder auftauchen und Schwierigkeiten machen, fällt dies in die Verantwortung der Schule bzw. der Lehrkräfte. Das widerspricht dem Bild von Schule als einem geschützten Raum, in dem sich Schüler*innen gefahrlos erproben können.

1 https://www.microsoftvolumelicensing.com/ProductResults.aspx?doc=Product%20Terms,OST&fid=87,45,88; schon die Suche nach den zutreffenden Nutzungsbedingungen gestaltet sich äußerst schwierig.
2 Wegen der großen Verbreitung bezieht sich dieser Text überwiegend auf Office 365. Fast alle Überlegungen gelten aber ganz ähnlich auch für andere webbasierte Dienste wie z.B. Zoom, Kahoot, etc.
3 https://www.heise.de/ix/meldung/Microsoft-veroeffentlicht-Datenschutzverpflichtung-fuer-Teams-4710766.html.

Datenschutzmythen

Office 365 ist jetzt erlaubt.

Hierzu gibt es verschiedene Meinungen: Das MSB hält den Einsatz von Office 365 zur Verarbeitung personenbezogener Daten für »datenschutzrechtlich bedenklich«[a], die Datenschutzbeauftragten in Thüringen[b] und Hessen[c] lehnen ihn ab. Weil auch bei der Verwendung von Office 365 personenbezogene Daten anfallen, ist klar, dass kein*e Kolleg*in und keine Schüler*in zur Verwendung gezwungen werden kann, selbst dann nicht, wenn z.B. ein Beschluss der Lehrer- oder Schulkonferenz vorliegt.

...aber ich möchte gar keine personenbezogenen Daten verarbeiten oder verwende nur Pseudonyme.

Schon die zum Anlegen eines Nutzer*innenkontos erforderlichen Daten (z.B. Mailadressen) sind personenbezogene Daten. Das Problem der in einem Dokument enthaltenen Metadaten ist auch bei Verwendung von Pseudonymen gegeben. Laden Schüler*innen Dateien ohne Account hoch, werden sie trotzdem durch technische Identifikationsmerkmale z.B. ihres Browsers, Betriebssystems oder Geräts erkannt.

Die Kommunikation ist verschlüsselt oder die Daten interessieren niemanden.

Interessant für die Konzerne sind v.a. die Metadaten. Die Verschlüsselung der Kommunikation ist daher zwar ein Fortschritt, aber bei weitem nicht hinreichend.

Die Schüler*innen (Kolleg*innen) nutzen Office 365 freiwillig.

Wenn tatsächliche eine informierte, freiwillige, jederzeit widerrufbare Zustimmung der Schüler*innen und ggf. der Erziehungsberechtigten vorliegt, wenn aus einer Nicht-Zustimmung keine Nachteile erwachsen und wenn sich die Schule an bestimmte Regeln hält (Abschließen eines Vertrags zur Auftragsdatenverarbeitung, Aufnahme in das Verfahrensverzeichnis), dann ist die Nutzung von Office 365 in der Tat möglich. Allerdings: Schon die Nicht-Zustimmung einer*s einzigen Schüler*in (Kolleg*in) wird die Schule dann vor erhebliche Probleme stellen, weil Verfahren und Prozesse doppelt eingerichtet werden müssen, damit niemandem ein Nachteil entsteht.

Office 365 ist der Industriestandard und daher unverzichtbar.

Informatorische Grundbildung zielt nicht auf die Bedienung eines spezifischen Programms, sondern darauf, die Konzepte und Ideen hinter Programmgattungen zu verstehen.

Die Schüler*innen und Eltern nutzen solche Dienste privat und haben nichts dagegen.

Schüler*innen und Eltern sind die Nebenwirkungen ihres privaten digitalen Handelns oft nicht bewusst, was für mehr differenzierte Thematisierung und Praxis in der Schule spricht. Ein bewusstes Einverständnis im privaten Raum rechtfertigt außerdem nicht den geschützten staatlichen Raum Schule für Konzerninteressen zu öffnen.

Andere Schulen/Unis nutzen auch Office 365...

...es ist aber fraglich, ob dort eine kritische Auseinandersetzung mit der Thematik stattgefunden hat.

a https://www.schulministerium.nrw.de/docs/Recht/Datenschutz/Fragen-und-Antworten/Sonstige-Fragen-zum-Datenschutzrecht-an-Schulen/index.html

b https://bildung.thueringen.de/schule/medien/datenschutz-in-schulen/

c https://datenschutz.hessen.de/pressemitteilungen/zweite-stellungnahme-zum-einsatz-von-microsoft-office-365-hessischen-schulen

In den USA bietet Microsoft nach eigenen Angaben[4] »personalisierte Werbung auf der Grundlage einer begrenzten Anzahl von einfachen, unempfindlichen und gesundheitsbezogenen Interessekategorien an, einschließlich Allergien, Arthritis, Cholesterin, Erkältung und Grippe, Diabetes, Magen-Darm-Gesundheit, Kopfschmerzen/Migräne, gesunde Ernährung, gesundes Herz, Männergesundheit, Mundgesundheit, Osteoporose, die Gesundheit der Haut, Schlaf und Vision/Augenpflege.« In Deutschland ist das nicht legal und wir müssen darauf vertrauen, dass es auch nicht geschieht – aber: Die Technik, mit der diese Informationen ermittelt werden, ist weltweit die Gleiche. Auch in Deutschland fallen diese Daten also an, sie werden nach Angaben des Anbieters lediglich (noch) nicht genutzt.

Tatsache ist: Einmal in die Hände privater Konzerne gelangte Daten bleiben dort für immer gespeichert. Schon heute sind die Missbrauchsmöglichkeiten enorm, sie werden in Zukunft mit Sicherheit noch wachsen. Wer sich die Mühe macht, die Nutzungsbedingungen und die Datenschutzerklärung[5] von Microsoft wirklich durchzulesen (über 100 Seiten!), wird schnell merken, dass das Erheben, Analysieren und Verwerten von Nutzer*innendaten integraler Bestandteil des Geschäftsmodells ist.

Außerdem können und werden Daten, die gesammelt vorliegen, von Kriminellen gestohlen. Wollen wir unsere und die Daten unserer Schüler*innen wirklich leichtfertig diesem Risiko aussetzen? Auch die rechtlichen und gesellschaftlichen Rahmenbedingungen können sich ändern. Sind wir ganz sicher, dass diese Daten jetzt und zu Lebzeiten nicht missbraucht werden können?[6]

4 Datenschutzrichtlinien unter https://privacy.microsoft.com/de-DE/PrivacyStatement; die Angaben zu den Gesundheitsdaten werden nur dann angezeigt, wenn Microsoft aufgrund der Browser- und Systemeinstellungen zum Schluss kommt, dass der Text auf einem Rechner im US-amerikanischen Markt gelesen wird.

5 https://privacy.microsoft.com/de-DE/PrivacyStatement; ausgedruckt mit Anzeige aller Informationen kommt man auf exakt 99 Seiten; selbst dann sind noch viele Angaben auf verlinkte Seiten ausgelagert.

6 Berühmt geworden ist z.B. der Fall der Firma *Clearview*, die illegal öffentlich zugängliche Fotos von Facebook und ande-

Rechtssicherheit und Datenschutzkonformität nach DSGVO bedeuten nicht, dass Daten vor solchen Praktiken sicher sind. Es bedeutet, dass man sein Einverständnis hierzu gegeben hat. Beides stellt also nur eine letzte Hürde dar, mit der Eltern bzw. Schüler*innen ein Veto gegen eine solche Verwendung ihrer Daten einlegen können. Selbst wer die Bestimmungen des Datenschutzes so gerade eben einhält, schützt nur sich selbst vor juristischen Konsequenzen. Ziel von Schule sollte aber ein effektiver Schutz der Daten von Schüler*innen und Kolleg*innen sein.

Lehrkräfte im deutschen Bildungssystem sollen Schüler*innen zur kritischen Auseinandersetzung mit gesellschaftlichen Entwicklungen und zur Mündigkeit erziehen. Dies ist übrigens auch zentrales Ziel des Mediencurriculums. Wenn man zentrale Schnittstellen der Arbeitsbeziehungen und Kommunikation zwischen Lehrer*innen untereinander oder zwischen Lehrer*innen und Schüler*innen in die Hände privatwirtschaftlicher Firmen legt, ist das eine beunruhigende gesellschaftliche Entwicklung, über die Politik, Verwaltung, Kollegien, Elternschaft und Schülerschaft diskutieren sollten.

Welche Konsequenzen drohen mir?

Für den Datenschutz an Schulen ist grundsätzlich die Schulleitung verantwortlich. Klar ist aber auch, dass alle Kolleg*innen auf die Einhaltung der Gesetze verpflichtet sind. Darauf haben sie sogar einen Eid abgelegt. Konkret bedeutet dies:

- Für Systeme, Programme etc., die von der Schulleitung verpflichtend eingeführt werden, trägt diese auch die Verantwortung. Wenn die Einführung gegen das Datenschutzrecht verstößt, haben Kolleg*innen die Pflicht, zu remonstrieren, d.h. zu protestieren. Dies erfolgt zunächst bei der Schulleitung, bei Protesten gegen Entscheidungen der Schulleitung direkt bei der Bezirksregierung. Empfehlenswert ist, mögliche Bedenken so zu äußern, dass diese später nachweisbar sind, etwa im Protokoll einer Konferenz oder durch eine Email an die Schulleitung, von der man eine Kopie behält.
- Wenn Systeme, Programme etc. zur freiwilligen Nutzung angeboten werden, trägt jede*r Kolleg*in selbst die volle Verantwortung.
- Eine strafrechtliche Verfolgung der Schulen und Kolleg*innen bei Datenschutzverstößen ist ausgeschlossen, es drohen aber zivilrechtliche und disziplinarrechtliche Konsequenzen (Schadenersatz, Schmerzensgeld). Weil die DSGVO sehr jung ist, gibt es hier noch keine Musterurteile. Welches Verhalten als grob fahrlässig gilt und daher sanktioniert werden kann, muss sich erst noch erweisen. In jedem Fall raten wir Kolleg*innen, gegen die rechtliche bzw. disziplinarische Schritte angedroht oder gar ergriffen werden, dringend, sich juristischen Rat z.B. über die GEW einzuholen. Noch besser ist es aber natürlich, sich gar nicht erst in eine angreifbare Position bringen zu lassen.
- Die Verarbeitung (und das meint bereits das bloße Anzeigen) von Schüler*innendaten an Privatgeräten der Lehrer*innen ist im Grundsatz verboten. Die Schulleitung kann eine Genehmigung zur Verarbeitung bestimmter Schüler*innendaten (Bilder, Audios nur mit Zustimmung der Schüler*innen bzw. Eltern) erteilen. Hierzu müssen die Kolleg*innen umfangreiche Selbstverpflichtungen zur Absicherung ihrer Geräte unterschreiben, die sie mangels IT-Kompetenzen häufig nicht einhalten können. Dies führt in ein unlösbares Dilemma, das nur die Bereitstellung digitaler Endgeräte durch den Dienstherrn lösen kann.

ren Seiten verwendet hat, um sie in einem System zur Identifizierung von Personen anhand von Kamerabildern zu verwenden, vgl. z.B. https://www.heise.de/newsticker/meldung/Bericht-US-Firma-sammelte-Milliarden-Fotos-fuer-Gesichtsdatenbank-4641569.html.

Welche Alternativen gibt es?

Sicher ist die Digitalisierung ein gesellschaftlicher Trend, der die Zukunft bestimmen wird. Zum gegenwärtigen Zeitpunkt sind aber nur wenige wirklich gute, ausgereifte Materialien für den digitalen Unterricht erhältlich. Das bedeutet, dass die Gestaltung von Unterricht mit digitalen Mitteln häufig unverhältnismäßig aufwändig ist und trotzdem oft nur mäßige Ergebnisse liefert. Außerdem besteht die digitale Ausstattung der Schüler*innen häufig nur aus einem Smartphone. Dieses hat zwar Internetzugang, ist aber sicher nicht zum Verfassen längerer Texte geeignet. Weiterhin fehlt in vielen Haushalten ein Drucker zum Ausdruck von Arbeitsblättern. Nicht ohne Grund gibt es bislang noch keine belastbaren Studien, die einen gesteigerten Lernerfolg durch digitale Methoden belegen.

Auch in Zeiten der Schulschließung gilt: Die einfachsten Lösungen sind häufig nicht die schlechtesten. Aufgaben aus Schulbüchern etwa sind von Fachleuten entwickelt und geprüft, die Materialien sind bei den Schüler*innen vorhanden.

Zugegeben: Die Arbeit z.B. mit Microsoft Teams ist zumindest aus Lehrer*innenperspektive komfortabel. Fraglich ist, ob das auch für die Schüler*innenperspektive gilt. Wenn Schulen dennoch die Einführung von digitalen Plattformen beschließen, gilt: Die Einführung einer Lern- oder Kommunikationsplattform kann nicht von der Schulleitung verordnet werden. Sie bedarf eines Beschlusses der Lehrerkonferenz und der Beteiligung des Lehrerrates. Wenn auch Schüler*innen oder Eltern die Plattform nutzen sollen, muss auch die Schulkonferenz zustimmen. Darüber hinaus unterliegt die Einführung einer Lernplattform der Zustimmung des zuständigen Personalrates. Außerdem bleibt die individuelle Nutzung freiwillig. Wer sich gegen die Nutzung entscheidet, darf dadurch keine Nachteile erleiden, indem er*sie z.B. von Teilen der Kommunikation ausgeschlossen wird.

Wo es vom Land angebotene Produkte gibt, sind diese in jedem Fall zu bevorzugen, weil davon ausgegangen werden kann, dass das Land die Datensicherheit und Rechtskonformität überprüft und garantiert. Einzelne Kolleg*innen und Schulleitungen müssen bei bestimmungsgemäßer Verwendung also keine juristischen oder disziplinarischen Konsequenzen befürchten. Zur Zeit ist bereits Logineo als Cloud, Kalender und Maillösung für Lehrer*innen erhältlich, eine Ausweitung auf Schüler*innen und die Anbindung der Lernplattform Moodle und eines Messengers sind angedacht.

Natürlich können auch Daten von der Plattform Logineo gestohlen werden. Aber weil ihre Software nicht auf Profilbildung ausgelegt ist und weil erhobene Daten nicht mit Daten von Drittanbietern angereichert und geteilt werden, ist das Risiko eines Missbrauchs deutlich geringer als zum Beispiel bei Office 365.

Fazit

Wir alle sollten uns die folgenden Fragen stellen:

*In welchem Verhältnis stehen Lehrkräfte zu ihren Schüler*innen? Sollen sie nur möglichst effizient Wissen vermitteln und abprüfen oder sollen sie auch für die Gestaltbarkeit gesellschaftlicher Entwicklungen sensibilisieren?*

*Erstreckt sich die Fürsorgepflicht der Lehrer*innen gegenüber ihren Schüler*innen auch auf den Schutz ihrer Daten?*

Soll Schule weiterhin ein geschützter Raum zur Persönlichkeitsentwicklung sein oder soll sie für ökonomische Verwertungsinteressen (weiter) geöffnet werden?

Unserer Meinung nach bedürfen Schüler*innendaten eines besonderen Schutzes und gehören daher nicht in die Hände von Privatfirmen. Schulen sollten echten Datenschutz auf höchstmöglichem Niveau anstreben und sich nicht mit einer gerade noch legalen Lösung zufriedengeben.

In der Pflicht ist hier vor allem die Ministerin. Wenn sie die Digitalisierung des Bildungswesens wirklich möchte, wird sie nicht umhinkommen, hierfür auch Geld in die Hand zu nehmen: Nicht nur für Geräte sowie deren sichere Einrichtung und Wartung, sondern auch für Plattformen, Programme und Inhalte, die definierten Qualitätskriterien entsprechen.

Die Digitalisierung der Schule soll und wird kommen. Aber wir sollten uns nicht von einem unreflektierten, von kommerziellen Interessen befeuerten Hype treiben lassen, sondern sie so gestalten, wie sie unseren didaktischen und pädagogischen Vorstellungen entspricht.

Fabian Blasius, Thorsten de Jong, Heike Wichmann
Kontakt: thorsten.de.jong@gew-nrw.de