

Meekijken op de devices van leerlingen

Scholen laten leerlingen steeds vaker gebruik maken van digitale apparaten zoals laptops, tablets of iPads. Tijdens de les willen docenten natuurlijk dat leerlingen opletten en niet stiekem spelletjes spelen of hun Facebook-account bijwerken. Ook bij een toets wil je zeker weten dat er niet 'digitaal gespiekt' kan worden.

De oplossing lijkt eenvoudig door op zo'n device software te installeren die precies bijhoudt wat een leerling doet. Maar mag dat wel? Op school en thuis hebben leerlingen recht op privacy. Zeker als de leerling een device gebruikt dat eigendom is van de ouders van de leerling. Hieronder lees je hoe je het meekijken op devices van leerlingen goed regelt.

Mag een school (preventief) berichten controleren op de telefoons van haar leerlingen?

Bij deze vraag is er sprake van een spanningsveld: aan de ene kant heeft de school de verplichting pesten tegen te gaan en te zorgen voor een veilig leerklimaat voor haar leerlingen. Aan de andere kant hebben die leerlingen ook recht op privacy. Het tegengaan van pesten en het bieden van dat veilige leerklimaat mag niet (volledig) ten koste van de privacy van leerlingen gaan. Wanneer een school besluit alle privé-gespreken op privé-telefoons van leerlingen te controleren dan raakt dat ook de privacy van alle leerlingen. Belangrijk aspect daarbij is dat een telefoon geen eigendom is van de school (anders dan bijvoorbeeld een door de school verstrekte iPad). Ook zijn lang niet alle leerlingen betrokken bij 'het voorval' (grensoverschrijdend gedrag), maar ze worden wel geraakt door deze maatregel. En wat doet een school met 'bijvangst' zoals expliciete berichten op een mobiele telefoon over een relatie? Of een filmpje waarbij een leerling tijdens de kerstvakantie een prullenbak op straat opblaast met vuurwerk (waarbij er dus geen relatie is met school)?

De wet stelt: bij het controleren van alle leerlingen op deze manier, is er sprake van "mass surveillance": het onbeperkt, zonder voorafgaande verdenking, controleren van persoonsgegevens met het doel overtredingen te ontdekken. Bij analyse van deze data kunnen ook patronen en verbanden in beeld worden gebracht. Deze methode komt overeen met methodes die de Engelse en Amerikaanse geheime diensten gebruiken om bijvoorbeeld terroristische activiteiten op te sporen.

In Europa staat privacybescherming hoog in het vaandel, en is privacy een grondrecht én mensenrecht. Een inbreuk daarop is alleen toegestaan als dat 1. wettelijk is geregeld en 2. (strikt) noodzakelijk is in een democratische samenleving (bijv. voor de openbare of nationale veiligheid). Over deze dubbele toets heeft het Europese Hof van Justitie heeft zich in meerdere zaken uitgesproken: mass surveillance is *disproportioneel* en een *onrechtvaardigbare* schending van de privacy.

Het door een school – zonder verdenking – bekijken van bijvoorbeeld alle berichten op een mobiele telefoon, komt eigenlijk overeen met waar het Europees Hof een uitspraak over heeft gedaan. Het controleren van alle telefoons is disproportioneel (niet in verhouding) tot het doel dat er mee bereikt moet worden:

1. Ten eerste is het structureel en stelselmatig bekijken van berichten op een mobiele telefoon door scholen niet wettelijk geregeld. We hebben in onze democratische rechtsstaat een organisatie aangewezen die, met de nodige democratische en juridische waarborgen, belast is met de opsporing van strafbare feiten: de politie. De waarborgen liggen daarnaast in de onafhankelijke rechtspraak. Bij controle door een school zijn deze waarborgen niet aanwezig.
2. Ten tweede is de vraag of deze 'opsporingsmethode' voor pesten (en mogelijk verdergaande onwenselijke gedragingen), strikt noodzakelijk is. Waarom beperkt de school zich niet tot het vragen (aan de ouders) om inzage als daar een concrete(re) aanleiding voor is? Of vraag ouders thuis die controle van de telefoon van hun kind uit te voeren. Op het moment dat een leerling (diens ouders) niet wensen mee te werken, kan de school zich altijd nog wenden tot de politie (wijk-/schoolagent). Ook valt de overweging dat bij grensoverschrijdend gedrag het slachtoffer (diens ouders) aangifte doet bij de politie.

Het stelselmatig zonder verdenking op deze wijze controleren van alle leerlingen gaat dus te ver en is in strijd met wet- en regelgeving. Sterker nog: het is een schending van de fundamentele rechten en vrijheden van de mens. Zelfs al zou een schoolreglement dergelijke opsporingsmethodes toepassen, mag dit dus nooit!

De enige ruimte die de wet geeft, is dat een school bij een concrete verdenking – op basis van een door de MR goedgekeurd schoolreglement o.i.d. – het gesprek met de leerling aangaat en om inzage in diens telefoon ‘vraagt’ (in afstemming met de ouders, die gaan over de privacy van leerlingen tot 16 jaar). De praktijk zal uitwijzen dat doorgaans – bij grensoverschrijdende filmpjes die worden gedeeld op school – er meestal wel (niet-betrokken) leerlingen zijn die het filmpje best aan de docent of directie willen laten zien. Als er geen medewerking wordt verleend, kan er contact worden opgenomen met de politie.

Mag de school de telefoons controleren van “verdachte” leerlingen?

Zie ook het antwoord hiervoor. Ook hier is sprake van hetzelfde spanningsveld: veiligheid versus privacy. Het grote verschil hierbij is dat niet alle leerlingen geraakt worden door het controleren van de telefoon van een enkele verdachte leerling. De ‘verdachte’ leerlingen heeft ook gechat met andere leerlingen die niet betrokken zijn. Uitgangspunt voor een school moet altijd de onschuldpresumptie zijn: een leerling is niet verdacht tot het tegendeel is bewezen. De school zal hierbij zelf de afweging moeten maken of de leerling (diens ouders) - op basis van vrijwilligheid - willen meewerken. En als er sprake is van strafrechtelijke gedragingen (verdenking van misdrijven) dan wordt de opsporing daarvan aan politie en justitie overgelaten. Een school is geen door de wet aangewezen opsporingsinstantie. Dan is het misschien beter om telefoons – in sommige gevallen - te verbieden, dan om politieagent te gaan spelen. Dus het inzien van een telefoon van een ‘verdachte’ leerling, kan je beter niet doen.

Mag een school tijdens de les tablets, computers of telefoons controleren?

Er geldt nét een iets andere regeling voor het klassikaal controleren van computers of tablets tijdens de lessen. Docenten hebben dan wel de mogelijkheid om bijvoorbeeld tijdens een toets preventief te controleren (meekijken op het scherm) of een leerling ‘aan het spieken’ is in andere software. Maar dat betekent dus niet dat een school het recht heeft om een volledige laptop of tablet te doorzoeken, of om doorlopende opnames (screenshots) te maken. Er is tegenwoordig software beschikbaar die het mogelijk maakt dat de docent op afstand de computers of tablets van leerlingen mee te kijken of om toegang tot het internet te blokkeren (bijvoorbeeld tijdens een toets). Bij het installeren van software op computers van leerlingen (hun ouders) moet natuurlijk vooraf toestemming zijn verkregen van de ouders. Dit kan ook goed uitgelegd en geregeld worden in een reglement. De reden voor dit type beheer, heeft dus een didactische achtergrond: om goed les te geven met een laptop of tablet, moet de leerling tijdens de les alleen het aangewezen lesmateriaal gebruiken en dus niet zitten Snapchatten.

Een methode als classroom-management lijkt meer aan de orde: via het wifi-netwerk wordt het gebruik van bepaalde sites of applicaties aan banden gelegd, of wordt de device van de leerlingen gecontroleerd. En als daar aanleiding voor is, kan een docent in zijn klas tablets ‘blokkeren’ zodat er alleen het betreffende leermateriaal gebruikt kan worden. Maar het standaard meekijken en afluisteren, zit meestal niet in dit classroom-managementsysteem.

En alternatief is om via het netwerk van de school het gebruik van sociale media te blokkeren (via het mobiele netwerk blijft dat altijd wel mogelijk).

Bedenk trouwens ook dat leerlingen erg vindingrijk zijn: als ze weten dat er gecontroleerd wordt op Whatsapp, zie je dat ze al snel de chatfunctie van Instragram of Snapchat zullen gaan gebruiken. Technisch kan je denken aan zogenaamde ‘whitelisting’ in plaats van blokkades: alleen datgene wat gebruikt mag worden is mogelijk.

In de praktijk is het beter om sterk in te zetten op bewustwording en voorlichting bij leerlingen. De school kan daarbij een grote bijdrage leveren door tijdens lessen aandacht te geven aan het respectvol met elkaar omgaan

en mediawijsheid. De brochure 'Sociale veiligheid op school' (https://www.kennisnet.nl/fileadmin/kennisnet/publicatie/Sociale_veiligheid_op_school_en_internet.pdf) gaat hier verder op in. De brochure 'Sociale media en schoolveiligheid' legt uit welk online gedrag eigenlijk strafrechtelijk strafbaar is

(http://archieff.kennisnet.nl/fileadmin/contentelementen/kennisnet/sociale_media/13_05_13_Sociale_Media_en_Schoolveiligheid.pdf).

Mag een school monitoring software installeren op de laptops van de school die leerlingen gebruiken?

Zie het eerste antwoord in deze e-mail. Als de laptop van school is, mag de school – binnen de wettelijke grenzen - voorwaarden verbinden aan dat gebruik.

Is het de bedoeling dat de leerling de laptop alleen voor schoolzaken gebruikt? Dan kun je je ook afvragen of je met die laptop überhaupt privéberichten moet versturen of op sociale media moet. De vraag is dan vooral wat de regels zijn omtrent het gebruik van de schoollaptop en of de genomen maatregelen proportioneel zijn (zie hiervoor).

Altijd alles structureel en stelselmatig controleren is niet proportioneel. Meekijken als daar een aanleiding voor is, of bij een vermoeden bij grensoverschrijdend gedrag, kan dat wel zijn. Ontbreken deze regels, dan is er sowieso sprake van een inbreuk op de privacy van de leerlingen.

Vermeldt dan duidelijk in de regels dat de laptop alleen voor schoolzaken gebruikt mag worden, dus niet voor bijvoorbeeld sociale media, illegale software of porno, én dat de school daarop een controle kan uitoefenen in het geval van misbruik. Dan mag de school wel bij een concrete aanleiding daarop controleren.

Maar let wel op dat een leerling door deze regels en controle, *thuis en in eigen omgeving en tijd*, nooit gecontroleerd mag worden. De regels gelden alleen op school en onder schooltijd. Denk ook na over alternatieven die de privacy minder schenden: beperkt meekijken via software, of via die software afdwingen dat een leerling alleen de door de docent aangewezen content kan bekijken.