IoT hubb skola

2019

IoT i skolan

Integritet, säkerhet och juridik

SVAMPEN - UNDERJORDENS HUBB

”Hos växter som samarbetar med en svamppartner hittar man dubbelt så livsnödvändigt kväve och fosfor jämfört med exemplar som bara suger upp ämnen ur jorden med hjälp av sina egna rötter… För att ingå partnerskap med någon av över tusen arter svampar måste trädet vara mycket öppet. Svampen tränger inte bara in och omsluter rötterna utan låter också sin väv vandra ut genom den kringliggande skogsmarken. Därmed överskrider den rötternas normala utbredningsområde och växer också över till andra träd. Här förbinder den sig med de andra trädens svamppartner och rötter. Ett nätverk uppstår med ett livligt utbyte av inte bara näringsämnen utan även information, till exempel om hotande insektsangrepp. Svampar fungerar därmed som skogens eget internet…”

Citat av Peter Woelhen ur boken *Trädens hemliga liv* (2017, 52-53)

Bilden på framsidan föreställer den delen av en svamp som går att se ovan jord. Den verkliga svampen, den som lever i flera årtionden består av ett upp till hundra kvadratmeter stort nät av underjordiska trådar. Detta nät är en del av ett större sammanhang eftersom svamptrådarna är anslutna till trädrötter som i sin tur hänger samman med andra svampindivider av olika arter som är förbundna med andra träd och andra växter. Nätverket är så tätt spunnet att en enda matsked mull kan rymma en mil svamptrådar.

RI.SE

IoT hubb skola

INTEGRITET, SÄKERHET OCH JURIDIK

Jan Hylén
Arbetsrapport arbetspaket 3:3. Januari 2019.
RISE - Research Institutes of Sweden

Denna rapport är framtagen inom projektet IoT Hubb skola som är en del av det strategiska innovationsprogrammet för sakernas internet (IoT Sverige), en gemensam satsning av Vinnova, Formas och Energimyndigheten.

SAMMANFATTNING

Projekt IoT-hubb skola har som övergripande mål att bättre nyttja möjligheter med IoT (Internet of Things) i skolan. Projektet ska inledningsvis leverera tre rapporter: en om state-of-the-art inom IoT för skola, undervisning och lärande (IoT i skolan - State-of-the-art kring undervisning och lärande 2019); en om behov avseende IoT i behovsägarnas verksamheter (IoT i skolan - Kartläggning och beskrivning av behov 2019); och en om de juridiska, säkerhetsmässiga och integritetsmässiga förutsättningarna för projektet. Föreliggande rapport avser frågor om juridik, säkerhet och integritet.

Individens integritet skyddas av de mänskliga rättigheterna och åtnjuter även grundlagsskydd. För elever tillkommer även Barnkonventionen som kommer att inkorporeras i svensk lag 2020. Den säger bland annat att det i alla åtgärder som rör barn i första hand bör beaktas vad som bedöms vara barnets bästa. Därför bör frågan om IoT-insatser i skolan inte bara bedömas ur ett integritetsperspektiv utan även ur ett bredare etiskt perspektiv.

En genomgående hållning i rapporten är att väga nyttan med olika åtgärder mot de risker åtgärderna kan medföra för individer, främst elever. Det finns områden där det är till nytta för eleverna att samla in, lagra och bearbeta data. Det tydligaste exemplet är kanske miljödata, att skolans lokaler har tillräckligt bra luft, bra ljus och att ljudmiljön är behaglig. Det har visats i studier att detta gynnar lärandet. Det är också icke-kontroversiellt att samla in sådan data.

Det finns också data som det är oetiskt att samla in och som det är förbjudet att lagra och bearbeta. Det gäller till exempel slentrianmässig insamling av biometriska data som är både olagligt och oetiskt att samla in.

De svåra frågorna uppstår i de fall där det kan finnas nytta för individen men där det är etiskt tveksamt. I sådana fall finns inga färdiga svar utan frågorna måste avgöras lokalt av berörda parter. Slutsatsen är att det åligger den som pläderar för att föra in IoT-enheter i skolan att öppet och transparent visa vilka data som ska samlas in och vad den ska användas till. Denna person har dessutom ansvar för att visa hur data lagras och bearbetas och att det inte föreligger risk att data används till andra syften än de angivna samt att de lagras säkert. Slutligen behöver man också kunna visa att eleverna inte utsätts för fysisk fara.

INNEHÅLLSFÖRTECKNING

1. INLEDNING

1.1 BESKRIVNING AV UPPGIFTEN

Projektet IoT hubb skola är ett Vinnovafinansierat projekt som syftar till att utveckla möjligheter och potential med IoT i skolan och i dess utbildningsmiljöer. Projektets övergripande mål är att bättre nyttja möjligheter med IoT i skolan genom upprättandet av en IoT hubb för skolan. Detta kommer att åstadkommas genom tre parallella processer;

- Ökad kunskap och förståelse om strategi, standardisering, modeller och juridik
- Iterativ testning och analys
- Utveckling och upprättandet av IoT hubb för skolan

Projektet sker i partnerskap mellan Eskilstuna, Falköping, Kungsbacka, Lidingö, NTI-gymnasierna, Skellefteå, Stadsmissionens skolstiftelse, Västervik, RISE, Stockholms Universitet, ATEA och Microsoft.

Arbetspaketet 3 ska genomföra en initial omvärldsanalys för projektet inom de områden som är av primär relevans. Det rör sig då om Internet of Things (IoT eller på svenska ”sakernas internet”) för byggnader, befintlig IoT i utbildningssektorn, och om den befintliga infrastrukturen av internettjänster i skolan. En behovs- och användaranalys genomförs för att skapa grundläggande möjligheter att prioritera vilka tester och demonstrationer projektet ska fokusera på, samt vilken IoT utveckling som är primär. Likaså var fokus ska ligga avseende guidelines och standardiseringsarbete.

Arbetspaketet ska leverera tre rapporter: en om state-of-the-art inom IoT för skola, undervisning och lärande (IoT i skolan - State-of-the-art kring

undervisning och lärande 2019); en om behov avseende IoT i behovsägarnas verksamheter (IoT i skolan - Kartläggning och beskrivning av behov 2019); och en om de juridiska, säkerhetsmässiga och integritetsmässiga förutsättningarna för projektet. Föreliggande rapport avser den tredje aspekten. Vidare är detta den första versionen av tre, den slutliga rapporten kommer att föreligga i juni 2020.

1.2 OM RAPPORTEN

Efter inledningen i avsnitt 1 kommer en kort redogörelse för arbetsmetoden bakom rapporten i avsnitt 2. I avsnitt 3 behandlas de integritetsmässiga och andra etiska aspekter av IoT i skolan och i avsnitt 4 de säkerhetsmässiga frågorna. I avsnitt 5 görs några korta avslutande reflektioner. Bilaga 1 behandlar de juridiska aspekterna av IoT i skolan. Bilagan är skriven av Fredrik Engström på Engström & Hellman Advokatbyrå AB.

1.3 AVGRÄNSNINGAR

Föreliggande rapport ska behandla de integritetsmässiga, säkerhetsmässiga och juridiska aspekterna av IoT i skolan.

Integritet avser, enligt Nationalencyklopedin, rätten för varje människa att få sin egenart och inre sfär respekterad och inte utsättas för störande ingrepp.[1] Rätten till integritet kan avse personlig integritet eller fysisk integritet. Rätten till fysisk integritet ligger i vårt fall nära frågan om säkerhetsmässiga aspekter av IoT och kommer i huvudsak att behandlas under detta avsnitt.

Individens rätt till integritet faller inom ramarna för mänskliga rättigheterna och åtnjuter ett grundlagsskydd enligt 2 kap. 6 § regeringsformen (RF). Även i artikel 8.1 Europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR) finns ett rättsligt skydd på området.

Att upprätthålla den personliga integriteten syftar dels till att skydda den enskilda individens rätt till ett privatliv, och dels till att skydda samhället som helhet genom att individer, vars integritet skyddas, kan nyttja demokratins rättigheter. Integritet är en förutsättning för att medborgarna ska kunna nyttja demokratins rättigheter och är kopplat till den fria åsiktsbildningen.

I sammanhanget bör det framhållas att EU:s dataskyddsförordning (GDPR) trädde i kraft den 25 maj 2018. Av GDPR framgår bestämmelser som aktualiseras vid behandlingen av personuppgifter och som därför kan bli av särskild vikt vid IoT-insatser.

Det är också av betydelse att Barnkonventionen inkorporeras i svensk lag 1 januari 2020. Där anges inte uttryckligen ordet ”integritet”. Däremot framgår det av artikel 16 Barnkonventionen att varje barns rätt till privatliv ska respekteras. Artikeln lyder: ”Inget barn får utsättas för godtyckliga eller olagliga ingripanden i sitt privat- och familjeliv, sitt hem eller sin korrespondens och inte

1 Nätupplagan

heller för olagliga angrepp på sin heder och sitt anseende. Barnet har rätt till lagens skydd mot sådana ingripanden eller angrepp."

Barnombudsmannen skriver att Barnkonventionen syftar till att ge barn, oavsett bakgrund, rätt att behandlas med respekt och att få komma till tals.[2] Bland annat ska det i alla åtgärder som rör barn i första hand beaktas vad som bedöms vara barnets bästa.

Mot denna bakgrund måste slutsatsen bli att om hänsyn ska tas till Barnkonventionen så räcker det inte att bedöma om olika IoT-insatser hotar elevens integritet, utan dessa insatser måste bedömas ur ett bredare etiskt perspektiv.[3] Avsnitt 3 i denna rapport kommer därför att behandla integritetsmässiga och andra etiska aspekter av IoT i skolan.

1.4 DEFINITION AV INTERNET OF THINGS

Det finns många olika definitioner av IoT, men de har alla gemensamt att de är relaterade till hur den fysiska världen integreras med den virtuella värld som utgörs av internet. En bred definition är att IoT är en global nätverksinfrastruktur, som kopplar unikt identifierade fysiska och virtuella objekt, saker och enheter genom utnyttjande av datainsamling, kommunikations- och manövreringsförmåga. IoT handlar dock inte bara om saker (”things”) utan även om relationerna mellan de dagliga föremålen som omger människor och människor själva.[4] Det kommer att framgå inte minst av avsnitt 4.1.

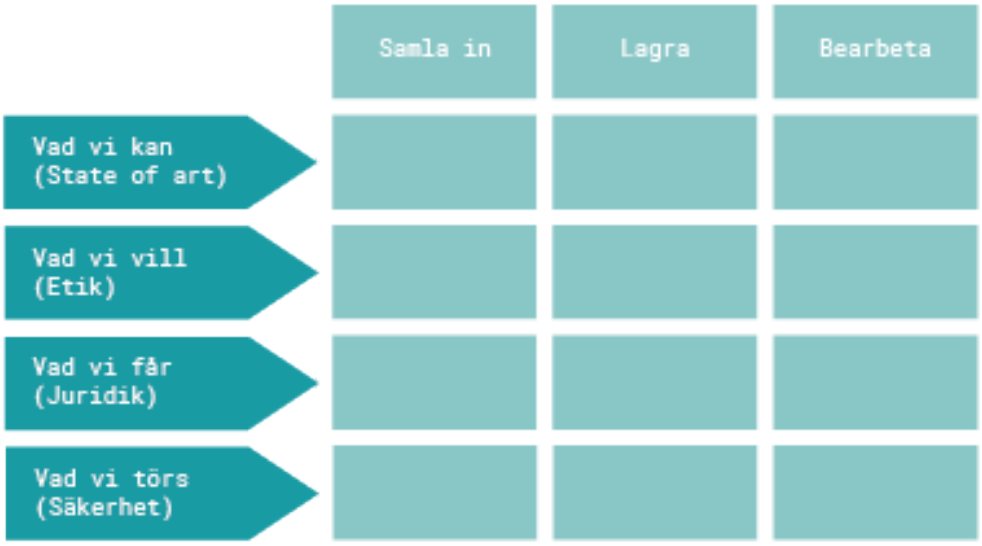
2 https://www.barnombudsmannen.se/barnombudsmannen/barnkonventionen/

3 För närvarande är det dock något oklart hur Barnkonventionen ska tillämpas i svensk praxis. Mot den bakgrunden har regeringen uppmärksammat behovet av vägledning i frågan (prop 2017/18:186 s. 90-91). Därför har regeringen gett i uppdrag åt socialdepartementet och professor Karin Åhman att ta fram en sådan vägledning t.om. den 31 maj 2019.

4 Internet of Things. Wikipedia: http://en.wikipedia.org/wiki/Internet_of_things

2. ARBETSMETOD

För att skapa systematik och överblick i arbetet med denna rapport har en enkel matris tagits fram. Den listar de olika frågeställningarna i det lodräta ledet och olika aspekter av varje frågeställning i det vågräta ledet.



Tabell 1: Aspekter på frågeställningar om integritet och säkerhet

Den första raden i matrisen avser vad som med IoT-teknik är tekniskt möjligt att samla in, lagra och bearbeta för olika typer av data. Dessa frågor behandlas inte i denna rapport utan i *IoT i skolan - State-of-the-art kring undervisning och lärande 2019*. Här fokuseras istället frågorna om vad vi med gott samvete vill samla in, lagra och bearbeta; vad vi rent juridiskt får samla in, lagra och bearbeta; samt vad vi av säkerhetsmässiga skäl törs samla in, lagra och bearbeta.

De juridiska, etiska och säkerhetsmässiga frågorna runt IoT är utmanande aspekter av en ökad teknikanvändning. I många fall är det också svårt att i IoT-kontexten skilja ut dessa aspekter från varandra eftersom man, för att kunna närma sig vissa av de integritetsmässiga och säkerhetsmässiga frågorna, kan behöva stöd i lagtexter. Och tvärtom, eftersom IoT i vissa delar har en mycket nära koppling till användarna så kan de etiska aspekterna inte tänkas bort när juridiska frågor och säkerhetsfrågor diskuteras. Likafullt kommer de tre aspekterna att behandlas i separata avsnitt i denna rapport. Detta för att göra texten överskådlig och enklare att ta till sig.

I det sammanhang som skolan utgör är det också nödvändigt att vara öppen och tydlig med vems integritet, säkerhet eller lagliga skydd som är utsatt. Det kan i olika scenarier vara:

- barnet eller eleven,
- vårdnadshavaren,
- läraren,
- övrig personal (till exempel lokalvårdare, vaktmästare, skolmåltidspersonal),
- skolledaren,
- skolhuvudmannen (skolchef eller motsvarande),
- politisk nämnd eller styrelse

Ibland kan det vara flera grupper samtidigt som är utsatta eller hotas. Men eftersom skolan är till för elevernas lärande, och eftersom de i de allra flesta fall är minderåriga och i många fall (i grundskolan) har en laglig skyldighet att befinna sig i skolan, är det i första hand elevens perspektiv som kommer att framhållas här. I förekommande fall kan även andra perspektiv behöva lyftas.

2.1 TEKNISK UTVECKLING

Den tekniska utvecklingen är snabb och det kan vara så att det redan finns eller håller på att utvecklas tekniska lösningar som gör att en del av resonemangen i föreliggande rapport är obsoleta. Några exempel på denna tekniska utveckling ges nedan.

På senare år har det av olika skäl blivit allt vanligare med övervakningskameror. Vanligen motiveras nya kameror med att säkerheten (mot rån, överfall, skadegörelse, terrorbrott eller liknande) behöver öka. Det brukar antas att det råder ett motsatsförhållande mellan personlig integritet och övervakning för ökad säkerhet, men det växer också fram tekniker som minskar denna motsättning eller till och med delvis gör den obsolet. Det är teknik som innebär att den enskilda sensorn eller kameran analyserar insamlad data direkt på det egna chippet och endast skickar iväg metadata. Eventuell personkänslig data lämnar alltså aldrig enheten.

I en finsk doktorsavhandling[5] beskrivs en teknik för övervakningskameror som skyddar privatlivet för individer genom att automatiskt kryptera bildregionerna där människor är närvarande i videon. Om en brottslig handling skulle äga rum, är det möjligt att med rätt behörighet selektivt avkryptera och avläsa data från individer av intresse för att analysera situationen. Detta möjliggör en analys av situationen utan att man behöver göra ingrepp i privatlivet hos personer som inte är relevanta i situationen, medan man kan använda data som bevis för eventuell brottslig verksamhet. Därmed är individernas integritet skyddad samtidigt som säkerheten upprätthålls.

Det ska framhållas att projektet IoT-hubb skola inte känner till om denna teknik bedöms annorlunda ur juridisk synvinkel än sensorer som sänder iväg all data. Vidare bör det framhållas att om sådan teknik skulle användas blir frågan om att skydda dessa enheter från intrång extra viktig.

En annan utvecklingslinje är vad som kallas federerat eller distribuerat lärande som innebär att system för artificiell intelligens (AI), vilka vanligen behöver samla stora datamängder som träningsdata. Inom hälso- eller skolsektorn är behovet av att samla stora mängder integritetskänslig data ett av de stora hindren för AI:s utveckling inom sektorn. Nu rapporteras om lovande försök att träna upp dessa system med data som aldrig lämnar sjukhusets eller skolans server.[6] Detta kallas federerat lärande. Tekniken innebär att det går att träna ett program med data lagrad på flera olika sjukhus utan att informationen någonsin lämnar sjukhusets lokaler eller berör ett teknikföretags servrar. Det görs genom att först träna separata program på varje sjukhus med de lokala data som finns tillgängliga och sedan skicka dessa program till en central server som kombinerar dem till en mastermodell. I takt med att varje sjukhus får mer data så kan den ladda ner den senaste mastermodellen, uppdatera den med sina nya data och skicka den tillbaka till den centrala servern. Under hela processen utbyts ingen rådata, bara programvaror, som inte kan ”köras baklänges” för att avslöja ursprungsdata. Tekniken är ännu i sin linda men kan vara ett viktigt steg på vägen för samhällssektorer som hälsa/sjukvård och utbildning.

Juridiken förändras också. Så kom till exempel i maj 2018 det nya dataskydds-direktivet GDPR. Det är till stora delar ännu oprövat. Detta är några skäl till att betrakta denna rapport som tillfällig och den kommer därför att successivt behöva uppdateras och förfinas.

5 Matusek, F (2014): Selective Privacy Protection for Video Surveillance. http://jultika.oulu.fi/files/isbn9789526204154.pdf

6 https://www.technologyreview.com/s/613098/a-little-known-ai-method-can-train-on-your-health-data-without-threatening-your-privacy/

3. INTEGRITETSMÄSSIGA OCH ANDRA ETISKA ASPEKTER AV IOT I SKOLAN

Denna rapport är inte författad av en filosof till professionen. Den gör heller inte anspråk på att beröra eller täcka in alla integritetsmässiga eller etiska aspekter av IoT i skolan. Den syftar till att lyfta ett antal frågeställningar som kan komma att beröras i projektet eller i en vidare kontext av användning av sensorer i skolan.

Gällande avgränsningar så är det viktigt att framhålla att föreliggande rapport inte handlar om att diskutera de etiska grundvalarna för ”den goda skolan”. Inte heller om mänskliga aspekter eventuellt går förlorade genom att sensorer förs in i skolmiljön eller om man genom att mätinstrument förs in i skolan endast får skenbart mer objektiva beslutssituationer. Syftet är mer begränsat: det handlar om att resonera om de etiska (och säkerhetsmässiga) överväganden som behöver göras av skolhuvudmän, rektorer och lärare runt elevers integritet och eventuellt andra etiska frågor runt införande av sensorer i skolan.

3.1 ETISKA ASPEKTER AV IOT I ALLMÄNHET

IEEE är världens största organisation för tekniker och ingenjörer. Den arbetar mycket med tekniska standarder men har även tagit fram ett etiskt ramverk för personer som arbetar med intelligenta och autonoma system.[7] Ramverket utgår från sex grundläggande regler:

7 https://standards.ieee.org/industry-connections/ec/autonomous-systems.html

Den etiska designen, utvecklingen och genomförandet av tekniker som intelligenta och autonoma system, som vanligen använder sig av sensorer, bör vara styrd av följande allmänna principer:

- mänskliga rättigheter: Se till att systemen inte kränker internationellt erkända mänskliga rättigheter.
- välbefinnande: Sätt människors välfärd i första rummet vid design och användning av dessa system.
- ansvar: Se till att de som designar och opererar dessa system är ansvariga för resultaten av systemens agerande.
- öppenhet: Se till att systemen fungerar på ett transparent sätt.
- medvetenhet om missbruk: Minimera riskerna för missbruk av systemen.

Dessa principer gäller alltså intelligenta och autonoma system och är ytterst allmänna. De ger viss men inte tillräcklig vägledning för hur man bör betrakta sensorer och IoT i skolmiljöer.

De typer av etiska problem som IoT aktualiserar är relaterade till bland annat autonomi (för saker och människor), säkerhet (dubbel användning, frihet, oberoende), frågor om jämlikhet, jämställdhet och rättvisa (som i sin tur har med tillgång till teknik, behandling, diskriminerande gränssnitt med mera att göra) och andra frågor.

I en rapport från en expertgrupp inom EU som diskuterat etiska frågor i relation till IoT, inleder man med att lista en samling karakteristika för IoT-tekniken som man menar har etiska implikationer.[8]

1. Allestädes närvarande och genomträngande (ubiquity and pervasiveness). Användaren är uppslukad av och nedsänkt i IoT, och det finns inga tydliga sätt att välja bort en IoT-miljö, förutom genom att dra sig tillbaka till en orörd natur och artefaktlös miljö.
2. Miniatyrisering och osynlighet. Datorn, som vi känner den med tangentbord och skärm, kommer gradvis att försvinna eller kommer att sluta vara det vi självklart menar med en dator. Datortekniken kommer att bli osynlig och försvinna alltmer ur människans synfält. Så även om funktionaliteten är framträdande och allestädes närvarande kommer den till stor del att vara osynlig. Det kommer att kräva särskilda designåtgärder för att göra tekniken synlig och mottaglig för inspektion, revision, kvalitetskontroll och ansvarsförfaranden.
3. Tvetydighet och ontologi. Skillnaderna mellan naturliga föremål, artefakter (det vill säga skapade föremål) och människor tenderar att suddas ut som en följd av att det blir allt enklare att omvandla enheter av en typ till en annan. Både i praktiken och på en begreppslig nivå (konceptuellt) kommer vi att behöva hantera tvetydigheter runt identitets- och systemgränser och hur verkligheten är beskaffad.

8 van den Hoven: Fact sheet- Ethics Subgroup IoT - Version 4.0. IoT Expert Group of DG Connect

4. Identifiering. Saker och objekt ges en elektronisk identitet genom märkning och nätverk av objekt. Vi kommer att behöva vänja oss vid det faktum att många, och till synes obetydliga, föremål och artefakter kommer att ha unika identiteter. Denna funktion är avgörande för idén om IoT. Frågor om vem som får tilldela, administrera och hantera dessa identiteter, vem som kommer åt dem och hur de påverkas oss i en globaliserad värld, är viktiga frågor som har med styrning och påverkan att göra.

5. Uppkoppling. Vi kommer att få en hög och aldrig tidigare skådad anslutningsgrad mellan objekt och personer i nätverk. Det innebär i sin tur en hög produktion av och överföring av data.

6. Medling och autonom handling. IoT-miljön ger sätt att utvidga och förstärka mänsklig handlingsförmåga. IoT-miljöer kan medföra spontana ingrepp vid mänskliga händelser och skeenden som inte direkt orsakade av människor och som är oförutsedda och oväntade (se vidare avsnitt 4.1 g). Människor kommer att agera i IoT-miljöer tillsammans och i samverkan med artefakter, anordningar och system, så kallade hybridsystem.

7. Inbäddad AI och AR. Smarta och dynamiska objekt, med framväxande beteende, inbäddning av artificiell intelligens och förstärkt verklighet (AR) samt kunskapsfunktioner som verktyg blir en (extern) förlängning av människokroppen och sinnena. På samma sätt som det i viss utsträckning redan anses nödvändigt att ha hjälp av traditionella datorer så kan det komma att uppfattas som nödvändigt att ha tillgång till den intelligenta IoT-miljön för att klara sig i samhället. Det kan liknas vid att många människor idag skulle känna sig kognitivt och socialt handikappade om de inte hade tillgång till sin mobiltelefon och sina sociala nätverkssajter.

8. Sömlös överföring. Interaktion, informationsflöden i en IoT-kontext, kommer att vara enkel, med potentiellt mycket låg transaktions- och informationskostnad.

9. Distribuerad kontroll. Kontroll och styrning av IoT-miljöer kommer inte att ske centralt, eftersom tekniken bygger på ett stort antal noder, nav och data. Styrning och övervakning måste därför ske i enlighet med teknikens distribuerade eller utspridda natur. Detta kommer att få konsekvenser för ansvarsfrågorna.

10. Big Data. IoT kommer att skapa, lagra, överföra och bearbeta enorma datamängder, på Exabyte-nivå och bortom.

11. Oförutsägbarhet och osäkerhet. En stegvis och inkrementell utveckling av IoT kommer att leda till nya beteenden utan att användaren har fullständig eller till och med relevant kunskap om IoT-miljön.

Dessa karakteristika kommer var för sig och i kombinationer att ge upphov till en oerhörd mängd etiska komplikationer, menar expertgruppen. Detta faktum är inte unikt för IoT utan i många avseenden gemensamt med många andra framväxande teknikområden. Det område som är tydligast kopplat till just IoT är annars integritets- och säkerhetsfrågor.

3.2 ETISKA ASPEKTER AV IOT I SKOLAN

Det är viktigt att framhålla att det inte enbart är risker förknippade med IoT-tekniken. Det finns en lång rad potentiella fördelar och vinster, både för individen (eleven, lärare) och för skolan som organisation. De organisatoriska fördelarna är sannolikt mindre relevanta ur ett etiskt perspektiv men en sammanvägd bedömning av de etiska aspekterna måste ta hänsyn till, och väga samman, fördelar som individer kan dra av tekniken med dess potentiella nackdelar och etiskt tveksamma konsekvenser.

Fördelar för elever – några exempel
Om sensorer i skolmiljön till exempel kan innebära bättre luftkvalitet eller ljudmiljö, så kan detta inverka positivt på elevernas inlärning. I en studie från 2015 visar ett antal brittiska forskare hur framför allt miljön i klassrummet påverkar lärandet. Studien bygger på mätningar i 153 klassrum i 27 skolor och resultaten för över 3 700 elever har uppmäts.[9] Dålig inomhusmiljö kan förklara 16 procent av variationen i elevernas kunskapsinhämtning, skriver forskarna. Ljus, temperatur och luftkvalitet har störst påverkan, men även andra miljöfaktorer spelar in. Att ha sensorer som mäter luftkvalitet, ljus och temperatur kan knappast anses diskutabelt ur etisk synvinkel. Tvärtom kan det närmast ses som en moralisk skyldighet skolhuvudmannen att erbjuda bästa möjliga inlärningsmiljö till eleverna, eftersom sämre inlärning kan ha livslånga negativa effekter för enskilda individer.

Å andra sidan kan otillbörlig manipulation eller hackning av sensorer i syfte att manipulera skolmiljön utsätta elever för fysisk fara som brand, giftiga ämnen i luften eller liknande. Här måste fördelarna av sensorerna vägas mot de nackdelar som den ökade risken innebär. Riskerna för att skolors sensorer ska hackas och manipuleras så att en brand bryter ut måste dock bedömas som små eftersom det krävs många saker på en gång för att åstadkomma detta:

- Kunskap (hackerkunskap)
- Syfte (terrorism)
- Apparater som kan överhettas eller annat som kan starta en brand. I det här exemplet gäller det att det är den yttre miljön som förändras så att apparaten eller motsvarande startar en brand, inte att själva apparaten har hackats. Om det är apparaten själv som hackats så är det inte de yttre sensorerna som kan läggas till last för händelsen.

Det är svårt att se ett troligt scenario framför sig där samtliga dessa betingelser föreligger. Därmed måste risken för att sätt upp miljösensorer sägas vara mycket låg och därmed kan skolhuvudmän sägas vara moraliskt skyldiga att med hjälp av sensorer optimera inlärningsmiljön i sina skolor.

Även andra typer av data, som inte är kopplade till enskilda personer, skulle kunna samlas in för att i olika avseenden utveckla skolan och skolmiljön. Ljudsensorer som är kopplade till belysningen så att belysningen sänks när ljudnivån blir för hög i en skolmatsal, är ett sådant exempel. Eleverna märker när ljuset sänks och inser att de måste sänka rösterna, vilket leder till en trivsammare matsalsmiljö.

9 Barrett, Zhang, Davies & Barrett (2015): Clever Classrooms, Summary report of the HEAD Project. Salford 2015.

Ett likartat exempel skulle kunna vara att använda ljudsensorer för att förstå om pojkar respektive flickor har mer taltid under lektioner genom att med artificiell intelligens analysera rösterna. Syftet i detta fall är att åstadkomma en jämnare könsbalans i taltid och därmed en mer jämställd skola. Återigen samlas inga persondata in, så ur etisk synvinkel borde exemplet vara till fördel för eleverna.

Det går också att tänka sig skolor som använder sensorer (inte kameror) för att kartlägga elevers fysiska rörelse i skolan för att kunna bygga upp modeller över var elever rör sig, var de söker studiero, var det uppstår trängsel med mera. Syftet kan dels vara att nyttomaximera skolans lokaler men också att kunna bygga bort delar (till exempel korridorer eller prång) där det uppstår irritation, trängsel och mobbningssituationer. Exemplet bygger återigen på att det är anonyma data som samlas in och som används för att förbättra studiemiljön och tryggheten för alla på skolan, vilket givetvis är moraliskt eftersträvansvärt.

En ur etisk synvinkel mer tveksam tillämpning är om en skola använder AI-förstärkt kameramjukvara för ansiktsigenkänning för att kunna identifiera om obehöriga är i skolmiljön eller inte. Fördelen i detta fall är en ökad trygghet för individen, sannolikt också en ökad känsla av trygghet. Nackdelen, och den etiskt tveksamma aspekten, är att övervakningen ökar. I detta exempel samlas dessutom biometrisk persondata in och som framgår av Bilaga 1 vore en sådan användning knappast laglig.

Frågan om teknik för ansiktsigenkänning i skolmiljöer är inte enbart en teoretisk frågeställning. Tekniken har testats i praktiken. IT-företaget Tieto har under 2018 genomfört ett experiment i en gymnasieklass i Skellefteå (21 elever) under en begränsad tid med automatisering av närvaroregistrering.[10] Bakgrunden var dels att manuell närvaroregistrering upplevdes ta mycket tid i anspråk för lärarna som istället kunde användas till undervisning och dels att man ville få högre kvalitet i sin närvarostatistik för att tidigare kunna reagera om elever hade hög frånvaro. Tanken var att kunna agera tidigare för att minska avhoppen från gymnasieskolan.

I projektet testades två tekniker parallell dels RFI-taggar (enkla chip som i busskort eller liknande)[11] och dels ansiktsigenkänning. Försöket var frivilligt att delta i och samtycke, som även vårdnadshavare fick ta del av, inhämtades från eleverna. All data lagrades lokalt i en dator inlåst på skolan som rensades i slutet av året när testet var över. Man gjorde intervjuer och enkäter med elever och personal innan start, under testet och i avslutning av testet.

Slutsatserna från undersökningen är att både elever och lärare kände sig bekväma med båda teknikerna. RFI-tekniken lägger ansvaret för registreringen i elevernas händer, men många elever glömde att ta med sig sin tagg vilket dels försämrade kvaliteten på statistiken och dels gjorde att eleverna kände sig förargade över att hela tiden behöva komma ihåg att ha med sig sin tagg. Ansiktsigenkänningen uppfattades av eleverna som en innovativ och ”cool” teknik. De var entusiastiska och ivriga att använda tekniken. Lärarna upplevde också att de behövde använda mellan 40-60 procent mindre tid till att föra närvarostatistik. I rapporten betonas att innan man permanent inför den här typen av teknik i skolmiljöer så måste ordentliga konsultationer med Datainspektionen genomföras. Man rekommenderar också att de etiska frågorna belyses djupare än vad som gjordes inför detta korta försök.

10 Tieto (2018): The Future Classroom Project. Do innovative technologies have the potential to transform presence registration? Skellefteå kommun och Tieto, 2018

11 Se https://sv.wikipedia.org/wiki/Radio_Frequency_Identification

En aspekt som inte diskuteras i studien är hur man bör hantera frågor runt samtyckes-klausulen. Enligt GDPR kan man behandla känsliga personuppgifter om de personer som uppgifterna gäller gett sitt uttryckliga samtycke, som var fallet i Skellefteå. Men den som gett sitt samtycke kan när som helst dra tillbaka detta. Om så sker så måste skolan inte bara sluta att registrera frånvaron med ansiktsigenkänning, utan också ta bort all data eller alla uppgifter om denna person från datasetet. Det innebär att om en elev mot slutet av terminen drar tillbaka sitt samtycke till att bli registrerad med ansiktsigenkänning så hamnar skolan i ett Moment 22 – man är dels skyldig att stryka eleven ur datafiler för frånvaro och dels skyldig att kunna redovisa elevens frånvaro under terminen. [12]

Ett sätt att möjligen undvika ett Moment 22 är att skolan hittar en teknisk lösning så att de biometriska uppgifterna lagras på ett annat ställe än den egentliga närvarodatan. Om dessa är skilda åt så bör det räcka att skolan tar bort de biometriska uppgifterna om en elev drar tillbaka sitt samtycke. Själva närvarodatan bör kunna sparas. Återigen bör det betonas att projektet IoT-hubb skola inte har den juridiska kompetensen att bedöma frågan, utan den bör diskuteras med Datainspektionen.

Learning analytics

Det utvecklas även IoT-teknik som är kopplad till läromedel och lärmiljöer, som bidrar till att samla in data om den enskilda elevens lärande (learning analytics) vilken kan analyseras dels automatiskt och dels av läraren. En etisk aspekt av learning analytics är övervakningsfrågan – elevens agerande både under lektioner och vid läxläsning eller liknande kommer att kunna följas på en betydligt mer detaljerad nivå än idag. Men eleven ”övervakas” redan av läraren och detta sker i enlighet med skollagen. Att denna övervakning blir mer effektiv kan knappast anses kränkande för individen, särskilt inte om det leder till ett bättre lärande. Detta gäller åtminstone så länge eleven är i skolan. En något mer tveksam situation uppstår när läraren kan se på vilka tider på dygnet eleven gör sina läxor. Det närmar sig en kartläggning av elevens (och familjens) vanor. Men inskränkningen i elevens integritet kan knappast kallas för allvarlig.

En annan aspekt av learning analytics är att en automatisk datainsamling som ger ett betydligt bredare underlag än dagens, sannolikt skulle skapa en mer likvärdig bedömning av elevernas kunskaper och prestationer. Detta förutsätter dock att det finns överenskommelser (standards) om vilka data som ska samlas in, och hur den ska presenteras, som följs av både myndigheter och konstruktörer av de lärmiljöer eleverna arbetar i. En mindre godtycklig och subjektiv bedömning skulle stärka elevernas rätt till en likvärdig bedömning.

Vid learning analytics så lagras och bearbetas elevdata.[13] Då är det viktigt att känna till vem, utöver läraren, som har tillgång till dessa data. Har till exempel ett läromedelsförlag eller app-utvecklaren tillgång till elevens data? Det kan knappast anses etiskt försvarbart att ett företag har tillgång till data som kan knytas till en enskild person. Men om företag använder anonymiserad data för att vidareutveckla produkter eller tjänster och att produktutvecklingen leder till att kommande elever lär sig mer eller lär sig effektivare, så lider inte enskilda elever skada. Tvärtom måste det anses vara en fördel att kommande elevgenerationer får bättre möjligheter än tidigare generationer.

12 http://missinfogeek.net/gdpr-consent/

13 För exempel på hur learning analytics kan användas i praktiken, se Vuorikari, Castaño Muñoz (Eds.) (2016). Research Evidence on the Use of Learning Analytics - Implications for Education Policy. Joint Research Centre Science for Policy Report; EUR 28294 EN; doi:10.2791/955210.

Redan idag arbetar de flesta elever i program eller system som samlar in data. Det gäller såväl Googles produkter som Microsofts Office-paket. Alla användare har sannolikt i användaravtal godkänt denna datainsamling men samtidigt vet varken föräldrar, skolhuvudmän eller myndigheter vilken data som samlas in, inte heller var eller hur den lagras och bearbetas.[14] Det bör särskilt påpekas att detta också gäller för de elever som är förpliktigade att gå i skolan och förutsätts använda skolans datorer och programvaror. Enligt GDPR så måste dessa data lagras på en server i Europa, men mer vet vi inte. I fallet med Googles och Microsofts produkter, så bör vi som användare kräva öppenhet och transparens från företagens sida om vilka data om elever som samlas in, lagras och bearbetas.

Elevnära sensorer

Vidare går det att tänka sig att ha sensorer som mäter elevers stressnivå, blodsockerhalt eller emotionella status. Med aktivitetsarmband kan puls, som är kopplad till stress, mätas. För diabetiker finns det sensorer som mäter insulinnivåerna och larmar om de avviker från normalvärdena. På motsvarande sätt borde det gå att ha sensorer som mäter om en elevs blodsockerhalt är för lågt och om eleven skulle behöva äta något för att kunna koncentrera sig bättre. Med kameror som registrera elevernas ansiktsuttryck skulle deras emotionella status kunna mätas, något som det finns exempel på vid kinesiska universitet. I samtliga fall kan man se att insamlad data skulle kunna vara mycket användbar, men i samtliga dessa exempel sätter både juridiken och etiken stopp. I detta fall kan ändamålet inte helga medlen.

En intressant fråga är dock hur en situation skulle bedömas där sådan data samlas in anonymt. Det skulle kunna ske genom att till exempel slumpmässigt dela ut 100 aktivitetsarmband bland eleverna på en skola och inte registrera vem som bär ett armband. Det skulle ge data om variationer i stressnivåer hos eleverna över skoldagen. På motsvarande sätt skulle man kunna ha kameror som registrerar ansiktsmönster, och därmed känslor, men inte har mjukvara för att känna igen olika individer. Sådan data skulle dock bli långt mindre värdefull men möjligen tillräckligt intressant för att samla in.

Slutsatsen av dessa exempel är att det inte bara ur juridisk synvinkel utan även i ett etiskt perspektiv är stor skillnad mellan å ena sidan insamlad data som kan knytas till en enskild elev och å andra sidan anonymiserad och aggregerad data. Men även behandling av anonymiserad data om elever kräver öppenhet om vilken data som lagras och bearbetas och hur den används.

14 För en djupare diskussion om samtycke se Lannerö, P. ”Plattformar och samtycke. Hur vi avtalade bort både det privata och det offentliga rummet – och hur vi kan få dem tillbaka”, i Andersson Schwartz, J. & Larsson, S: (2019) Plattformssamhället. Den digitala politik, innovation och reglering. Fores.

3.3 INSAMLING BEARBETNING OCH LAGRING AV DATA UR ETISK SYNVINKEL

Etiskt och integritetsmässigt tveksamma situationer kan även uppstå vid bearbetning av data. Det gäller till exempel om olika, var för sig harmlösa uppgifter, sammanställs på ett sätt som kan utsätta eleven för fara att bli kränkt, utsatt för orättvis behandling eller liknande. Det innebär att det inte bara är insamlingen av data som bör bedömas ur integritetsmässiga och säkerhetsmässiga perspektiv, utan även bearbetningen av data. Detsamma gäller i hög grad lagringen av data.

IoT genererar mycket data som ger möjlighet till mer komplexa och detaljerade bedömningar. Med mängden data ökar också komplexiteten i att tolka data, att förstå vad den egentligen säger. Därmed ställs stora krav på att resultaten visualiseras på ett korrekt men samtidigt lättillgängligt sätt, både av individen som berörs men också av lärare, skolledare och beslutsfattare av olika slag. Annars finns risk för feltolkningar med fel beslut som följd. Även av dessa skäl är det viktigt med tillit och öppenhet. Berörda personer måste kunna ha insyn i vilka data som samlas in, hur de bearbetas och visualiseras för att kunna föra en initierad diskussion om resultatens relevans och tillförlitlighet. Transparens är en förutsättning för att insamling och bearbetning av data av det slag som diskuteras här, ska kunna anses etiskt rimlig. Blir processen sluten finns det risk att vi antingen blir teknikens fångar eller att det uppstår brist på tillit och motstånd.

Många av de etiskt tvivelaktiga situationerna med IoT uppstår i samband med lagring och bearbetning av data. Detsamma gäller säkerhetsmässiga aspekter på IoT. För att undvika upprepningar förs diskussionen om lagring och bearbetning av data i kommande avsnitt som behandlar just säkerhetsaspekter av IoT.

4. SÄKERHETSMÄSSIGA ASPEKTER AV IOT I SKOLAN

De säkerhetsmässiga aspekterna av IoT i skolan är av två slag: dels risker för fysisk fara och dels risker för att data används på sätt som inte ursprungligen var avsedda. Det kan i sin tur bero på att data inte samlats eller lagrats på ett säkert sätt.

Som framgick av tidigare resonemang är sannolikt de fysiska riskerna med IoT i skolan små. Mindre miljöpåverkan genom otillbörlig manipulation av sensorer, som att sänka eller öka temperaturen i lokalerna, skulle kunna orsaka obehag och besvär men knappast fysisk fara.

4.1 RISKER VID INSAMLING AV DATA

Risker vid insamling av data skulle kunna uppträda om någon till exempel otillbörligt påverkar sensorer i hårdvara eller mjukvara som eleverna använder. Det skulle kunna innebära att en elevs prestationer eller resultat inte fångas på rätt sätt, vilket i sin tur skulle kunna påverka eleven både på kort sikt (att eleven inte erbjuds stöd som den har rätt till) och på lång sikt (genom att betygen blir missvisande för elevens kunskaper).

I en rapport från ett europeiskt forskarnätverk om policy-frågor runt IoT, lyfts sju nyckelområden fram runt säkerhetsfrågor som berör IoT.[15]

15 Internet of Things. IoT Governance, Privacy and Security Issues. European Research Cluster on the Internet of Things, 2015.

a. Kontextbaserad säkerhet och integritet

Det handlar till exempel om risken att övervakningskameror tar bilder med låg kvalitet vilket kan ge ”felaktiga eller falska resultat” och att fel person blir anklagad för intrång i någon av skolans lokaler. Detta kan i sin tur kan påverka trovärdigheten för övervakningssystemet, förutom det övergrepp som blir följden av att fel individ anklagas.

Utrustning som används i annat syfte än det ursprungligt avsedda kan ge liknande resultat.

b. Cyber-fysiska system och IoT

Detta område handlar om att det allt oftare finns en tät koppling mellan (system av) datorer och den fysiska miljön. Det kan gälla sensorer för övervakning av människors hälsa eller för ökad säkerhet eller ergonomi på arbetsplatser, smarta nät för energifördelning och intelligenta transportsystem. Detta är system som påverkar människors hälsa och fysiska säkerhet och om de fallerar eller missbrukas så kan fysisk skada uppstå. I en skolmiljö skulle det kunna gälla möjligheter att felaktigt utlösa brandlarm så att sprinklersystem sätts igång, eller tvärtom att överhetta produkter för att starta bränder.

Huvudproblemet i detta fall är att dessa enheter är mer och mer inbyggda i vår vardag, samtidigt som de inte alltid har tillräcklig kapacitet att implementera avancerade säkerhetsskyddslösningar. Utmaningarna handlar om skalbarhet (miljarder enheter att skydda), harmonisering och homogenitet (olika protokoll och tekniker).

c. Datakorrelation och informationshämtning

IoT genererar data i olika sammanhang. Dessa data kan kombineras för att få fram ny information som inte tidigare var tillgänglig. Men möjligheten att komma åt denna stora mängd data möjliggör emellertid också generering av mer komplexa och detaljerade användarprofiler. Denna fråga behandlas vidare under avsnitt 4.2.

d. Anonymisering av användarnas data i en distribuerad och mobil miljö

Möjligheten till att korrelera eller samköra data leder över till frågan om anonymisering. Det finns två huvudsakliga utmaningar för anonymisering i IoT. En är relaterad till svårigheten att anonymisera data under insamlingsprocessen (till exempel från sensorer) eftersom detta skulle kräva ytterligare teknik (med ökad enhetskostnad). En annan är risken för (åter-)identifiering av individen från mängden av aggregerade och anonymiserade data. Även denna punkt behandlas vidare under avsnitt 4.2.

e. Risken för hackning relaterat till det stora antalet sensorer

Det finns risk att enheter eller sensorer blir hackade och stängs av eller agerar annorlunda än vad som varit den ursprungliga avsikten. Det kan leda till fysisk fara. Enheter som hackas kan också leda till att data kommer i händerna på obehöriga. Frågan ligger nära punkt b) ovan, men här är det inte hela cyber-fysiska system som avses utan mindre sammanhang. De fysiska riskerna är desamma som i b) och när antalet sensorer växer så ökar också risken för att någon eller några av dem blir manipulerade eller går sönder.

f. Fysisk tillgänglighet för enheter

IoT innebär vanligen att det finns många små anslutna sensorer, givare eller manöverdon inbäddade i den fysiska miljön. Per definition kommer dessa enheter att vara fysiskt tillgängliga för personer som vill skada dem eller använda dem på olika sätt för att kränka integriteten eller tillförlitligheten hos ett IoT-system. Antalet enheter i sig och deras reducerade kapacitet gör det väldigt svårt att upptäcka manipulering och kontrollera att de faktiskt fungerar som de ska.

Denna utmaning är relaterad till svårigheten att med säkerhet veta om enheten arbetar i rätt sammanhang (till exempel att de inte flyttats eller att miljöförhållandena inte förändrats lokalt), om de varit föremål för hackning och så vidare.

g. Överlämning av mänsklig makt till IoT

IoT öppnar för sömlösa hybridiserade interaktioner mellan människor och olika smarta och dynamiska objekt som kan innebära framväxande men oplanerade skeenden. Det kan innebära ofrånkomliga, oförutsedda och oväntade resultat. Det kan gälla olika ”artefakter” som bärbara sensorer (smarta klockor), anslutna medicinska anordningar (hälsoarmband) och andra implanterbara anordningar (implanterade chip) som blir förlängningar av människokroppen eller sinnet och som ökar gränssnittet mellan människor och omgivningen. Det är inte alltid denna typ av artefakterna uppfattas som agenter, det vill säga handlande enheter, av användarna. Frivilligt eller ofrivilligt kan användaren behöva förlita sig på tekniska artefakter för att klara av de sysslor som tekniken är avsedd att hjälpa honom eller henne med. Man brukar tala om ”agens”, att ett tekniskt system tar beslut och utför handlingar.

Genom att flytta eller delegera mänsklig autonomi och handlingskraft till IoT-föremålet finns det en potentiell risk för användarens integritet och säkerhet. I vissa fall kommer artefakterna att agera på användarens villkor, men vissa artefakter kan komma att fungera utifrån deras utvecklares världsbild, intentioner och intressen snarare än användarens. Det sker ofta omedvetet från utvecklarens sida.[16]

I skolans fall kan detta handla om att det inte blir eleven eller läraren som styr eller föreslår vad nästa steg i elevens arbete ska vara, utan en programvara. Om ett system som har ”agens” används men inte är tränat under svenska förhållanden så kan systemets inlärda stöd föreslå åtgärder som går i en annan riktning än vad den lokala lärarens eller den svenska läroplanens menar är det riktiga. I ett sådant fall föreligger ett allvarligt problem för utbildningssystemet men givetvis i första hand för den enskilda eleven.

Biometriska data
Särskilt känsliga data är så kallade biometriska uppgifter. I artikel 4 GDPR definieras biometriska uppgifter så här: ”personuppgifter som härrör från specifik teknisk bearbetning avseende fysiska, fysiologiska eller beteendemässiga egenskaper hos en fysisk person som tillåter eller bekräftar den fysiska persons unika identifiering”.

16 På Youtube finns filmer som visar hur tvålautomater enbart ger tvål till ljushyade händer medan mörka händer som sträcks fram blir utan tvål, se https://www.youtube.com/watch?v=8PlUf30rvyA. Systemet reproducerar normer och värderingar som finns i den träningsdata det haft tillgång till. Man brukar tala om maskinlärningens konservativa sida. För ytterligare läsning se: Larsson S (2018): Sjyst AI och normativ design, i Akenine & Stier (ed): Människor och AI. En bok om artificiell intelligens och oss själva. Books on Demand, Stockholm.

Det kan gälla fingeravtryck som används för att låsa upp mobiltelefonen, igenkänning av hörselgången genom hörlurarna[17] eller ansiktsigenkänning som i exemplet från automatisk närvaroregistrering ovan.

Det finns många fördelar med att använda biometri. Känsligheten hos informationen gör det till ett mycket säkrare sätt att verifiera någons identitet – det finns inget sådant som svaga fingeravtryck eller att någon kan knäcka ansiktsigenkänning som man knäcker ett lösenord. Som en del av ett autentiseringssystem med flera faktorer kan biometri minska risken för att hackare bryter sig in i användarnas konton.

Problemet med biometriska data är om uppgifterna blir stulna. Vanliga lösenord eller kreditkort med mera kan bytas ut, men man kan inte byta ut sitt ansikte, sitt fingeravtryck eller sin hörselgång. Skadan blir därmed oerhört mycket större och försiktigheten med att samla in, lagra och bearbeta biometriska data måste vara ännu större än vid annan data.

Detta framgår också tydligt av artikel 9 GDPR att det krävs särskilda undantag för att behandla biometriska uppgifter (se Bilaga 1, framför allt avsnitt 3).

4.2 RISKER VID BEARBETNING OCH LAGRING AV DATA

De risker som finns i samband med bearbetning av data gäller framför allt

- att data används i nya eller andra syften än de ursprungligen angivna,
- att samkörning av uppgifter som kanske var för sig är harmlösa kan ge ny information som kan utgöra ett hot mot eleven,
- att data inte anonymiseras under insamlingsprocessen (till exempel från sensorer) eftersom detta skulle kräva ytterligare teknik (med ökad enhetskostnad).
- att individer kan (åter-)identifieras med hjälp av mängden av aggregerade och anonymiserade data.

Data skulle både medvetet och omedvetet kunna användas i andra syften än de ursprungliga. Det är för att hindra detta som dataskyddsförordningen GDPR har tydliga regler om att ändamålet med uppgiftsinsamlingen ska vara tydligt. Medveten användning av data i andra syften än de ursprungligen avsedda är alltså olagligt men kan givetvis förekomma ändå.

Med ökad insamling av olika slags data ökar också möjligheterna att samköra dem, det vill säga korrelera dem med varandra. På så sätt kan mönster klarläggas som de ingående uppgifterna var för sig inte alls kan visa. Det kan vara till fördel för individen som framgick av exemplet om learning analytics. Men det kan också missbrukas. Ett exempel kan vara att elever som har skyddad identitet och någon form av hotbild mot sig skulle kunna identifieras och deras tider eller skolschema skulle kunna avslöjas. Samma problem kan uppstå genom att individer kan återidentifieras med hjälp av mängden av aggregerade och

17 Se till exempel https://www.bbc.com/news/technology-35766069

anonymiserade data. Trots att data avidentifierats kan man ibland med hjälp av mängden data hitta sådana mönster att enskilda elever kan identifieras.

Alltför billiga och enkla sensorer skulle kunna skapa säkerhetsproblem genom att de inte anonymiserar data under insamlingsprocessen eftersom detta skulle kräva ytterligare teknik och därmed högre kostnader. Då kan motsvarande problem uppstå som i exemplen ovan.

Risker med lagring av data
Vanligare än att diskutera risker med bearbetning av data är att lyfta fram risker i samband med lagring av data. Arbete för att skydda lagrade data kallas informations- eller datasäkerhet. Informationssäkerhet har till syfte att bevara sekretess, integritet och tillgänglighet av data. Det handlar om att åtgärder vidtas för att hindra att information läcker ut på fel ställe, förvanskas eller förstörs, och för att informationen ska finnas tillgänglig när och där den behövs. Det finns en globalt erkänd standard för informationssäkerhet, kallad ISO 27000. Dataskyddsförordningen GDPR ska också medverka till att skydda persondata för alla medborgare i EU. Genom GDPR får medborgarna utökade rättigheter såsom rätten att bli glömd, ändra felaktiga uppgifter eller få sin data flyttad.

En viktig aspekt är var, rent geografiskt, som informationen lagras. Det blir allt vanligare att använda så kallade molntjänster för att lagra data. I praktiken innebär en molntjänst att data lagras på en server som kunden inte vet var den finns. Lagringstjänsten erbjuds över internet vilket för kunden medför fördelen att man själv varken behöver ha särskilt kraftfulla datorer eller IT-kunnig personal. Men samtidigt som kundens ansvar för underhåll minskar blir det svårare att kontrollera att underhåll och säkerhet sköts som sig bör. Dessutom tillkommer, i synnerhet om tjänsterna tillhandahålls utomlands, problem med ansvarsfördelning, med hur lagarna i de berörda länderna samverkar och möjligen hur kommunikationerna mellan servern och användaren av data kan skyddas (då man inte kan begränsa dem till ett skyddat intranät). En nyligen stiftad amerikansk lag gör det svårt för svenska myndigheter att använda amerikanska molntjänster, menar en juridisk expertgrupp från ett antal svenska myndigheter kallad eSam.[18]

Ett stort problem med molntjänster, oavsett leverantörens geografiska position, är risken för dataintrång. Det har blivit allt vanligare att nyhetsmedia rapporterar om stulna kreditkortsuppgifter och liknande intrång. Motsvarande intrång kan hota integriteten och säkerheten för eleverna. Den motåtgärd som leverantörerna kan ta till är främst kryptering som gör data oläslig för tredje part. Men eSam pekar i sitt arbete på att det i praktiken inte har kunnat verifieras att krypteringsmekanismer som används ger tillräckligt skydd.

eSam ser ändå positivt på användningen av molntjänster.[19] De menar att molntjänsterna är en förutsättning för en ökad digitalisering av den offentliga förvaltningen. Samtidigt säger de att det inte går att ge generella råd om molntjänster bör användas eller inte, det är upp till varje organisation att göra sin egen bedömning. eSam uppmanar den som står inför ett beslut om molntjänster att noggrant analysera vilken typ av information som ska hanteras i molntjänsten och att göra nödvändiga risk- och konsekvensanalyser.

18 http://www.esamverka.se/nyheter/nyheter/2018-12-14-esams-rattsliga-uttalande-har-satt-molnfragan-pa-agendan.html. Se http://www.esamverka.se/download/18.290a0225166bfafb714c0c7a/1542007824143/eSam%20-%20Ra%CC%88ttsligt%20uttalande%20om%20ro%CC%88jande%20och%20molntj%C3%A4nster.pdf

19 Ibid

eSams resonemang visar att vi ständigt hamnar i situationer där vi måste göra en avvägning mellan risk och nytta. Det är dock lätt hänt att det blir individen som får stå för risken medan gruppen eller samhället tillgodogör sig nyttan. Det är därför lagstiftningen blir så viktig. I denna rapport har vi även elevperspektivet att ta hänsyn till och vad som Barnombudsmannen med hänvisning till Barnkonventionen kallade det som bedöms vara ”barnets bästa”. Tyvärr går det inte heller att göra det enkel för sig genom att säga att sensorer och IoT med hänsyn till barnens bästa inte har i skolan att göra. Vi har sett ett antal exempel där det uppenbart är till barnens och elevernas fördel att det finns sensorer. Det innebär att vi inte kommer ifrån att göra de svåra etiska övervägandena.

Alternativet till att använda molntjänster är att lagra data lokalt. Så gjorde man till exempel i försöket med ansiktsigenkänning i Skellefteå (se avsnitt 4.2). Även i ett sådant fall måste man tillse att det finns strikta rutiner för vem som har tillgång till lokalen och den lokala servern. Vi påminner återigen om att det är biometriska data som lagras i detta fall, vilket är extra riskfyllt.

En helt annan typ av risk vid lagring är att data förloras. Denna risk föreligger både vid lokalt lagrad data och vid användning av molntjänster. Det kan till exempel ske genom att servern inte underhålls som den ska eller att det inte har tagits kopior (back-up) av data. Vid molntjänster är risken att företaget bakom tjänsten begår misstag så att data förloras eller går i konkurs. Eftersom företagen som säljer molntjänster är experter på detta så är risken att de förlorar data sannolikt mindre än vid lokalt lagrad data, men den finns.

För elever kan det vara till stor skada att till exempel uppgifter om provresultat eller liknande försvinner. Men den typ av data som vanligen samlas in genom sensorer är knappast av detta slag. Däremot skulle förlust av data som skulle ha använts för learning analytics kunna innebära problem för elever, inte fysisk skada men väl att deras möjligheter till rätt typ av stöd och hjälp minskar.

5. AVSLUTNING

Baserat på de resonemang som finns tidigare i denna rapport kommer vi avslutningsvis att försöka göra en samlad bedömning.

Det finns områden där det är till nytta för eleverna att samla in, lagra och bearbeta data. Det tydligaste exemplet är kanske miljödata, att skolans lokaler har tillräckligt bra luft, bra ljus och att ljudmiljön är behaglig. Det har visats i studier att detta gynnar lärandet. Det är också icke-kontroversiellt att samla in sådan data.

Det finns också data som det är oetiskt att samla in och som det är förbjudet att lagra och bearbeta. Det gäller till exempel slentrianmässig insamling av biometriska data. I dessa fall råder ingen tvekan – datainsamlingen är både olaglig och oetisk och ska inte genomföras.

De svåra frågorna uppstår i de fall där det kan finnas nytta för individen men där det är etiskt tveksamt. Ett sådant fall kan vara exemplet med ansiktsigenkänning vid närvarokontroll. Rent juridiskt finns det möjlighet att genomföra detta genom att inhämta samtycke, vara försiktig med hur data lagras med mera. Men som redan diskuterats finns det stora risker om biometriska data kommer på avvägar. Samtidigt gjorde lärarna i denna studie uppskattningen att de tjänade omkring 10 minuter per lektion på att slippa registrera närvaron, tid de istället kunde ägna åt eleverna. De upplevde att de hade bättre kontroll över situationen och att lektionerna fick högre kvalitet. Som projektgruppen bakom studien själva påpekade så finns det alltså både nytta och risker med metoden och om en skola vill genomföra liknande åtgärder så bör de pröva frågan noga såväl ur juridisk som ur etisk synvinkel.

En annan typ av frågor gäller säkerheten. Här pekas det på att blotta antalet sensorer kan utgöra en risk eftersom de genom sin (växande) mängd är svåra att ha kontroll över. Den moraliska fråga som uppstår av detta konstaterande är om

det är etiskt acceptabelt att medverka till att öka antalet sensorer i skolmiljön, eller om det enda rätta är att helt avstå? Det bör åtminstone vara så att den som argumenterar för fler sensorer i skolan måste kunna visa att de tillför värde, ger nytta för eleverna. Något annat skäl kan inte finnas att öka antalet IoT-enheter.

Vidare kan sensorer vara farliga genom att de samverkar med den fysiska miljön, men där är det svårt att hitta några gångbara exempel från skolmiljön.

Slutsatsen blir att det åligger den som pläderar för fler IoT-enheter i skolan att öppet och transparent visa vilka data som ska samlas in och vad den ska användas till. Det åligger vidare denna person att visa hur data lagras och bearbetas och att det inte föreligger risk att data används till andra syften än de angivna samt att de lagras säkert. Slutligen behöver man också kunna visa att eleverna inte utsätts för fysisk fara.

Därmed skulle den matris som beskrevs i avsnitt 2 kunna kompletteras med en ytterligare rad som berör frågan om vad för data vi bör samla in, lagra och bearbeta.

	Samla in	Lagra	Bearbeta
Vad vi kan (State of art)			
Vad vi vill (Etik)			
Vad vi får (Juridik)			
Vad vi törs (Säkerhet)			
Vad vi bör			

Tabell 2: Aspekter på frågeställningar om integritet och säkerhet med en ytterligare rad som berör frågan om data.

6. KOMMANDE ARBETE

Som nämndes inledningsvis är detta den första i en serie om tre rapporter. Kommande rapporter skulle kunna behandla frågor som:

- Hur länge kan vi, får vi, vill vi och törs vi lagra data?
- Vem bär ansvaret för i (av) skolan lagrad data? Vilket ansvar har skolan respektive skolhuvudmannen här?
- Vad händer när den geografiska gränsen mellan skolan och hemmet suddas ut som vid fjärrundervisning, eller när sensorer registrerar data utanför schemalagd tid?
- Vem får hämta ut (och lägga till?) data från skolans sparade data? Och under vilka förutsättningar får detta göras?
- Vad sker juridiskt, säkerhetsmässigt och kanske även etiskt i relation till uppdateringar (inte minst automatiska uppdateringar) av mjukvara? Vem har ansvar för att ha kontroll över att sensorerna inte gör annat än vad som ursprungligen var tänkt och godkänt?
- Frågor runt övervakningssamhälle, tillit, transparens i relation till skolplikt.

Den exakta inriktningen styrs av hur projektet IoT-hubb skola utvecklas och vilka frågor som projektmedlemmarna har behov av att diskutera.

REFERENSER

Akenine & Stier (ed): *Människor och AI. En bok om artificiell intelligens och oss själva*. Books on Demand, Stockholm 2018.

Andersson Schwartz, J. & Larsson, S (2019): *Plattformssamhället. Den digitala politik, innovation och reglering*. Fores 2019

Baldini et al. (2015): *Internet of Things, IoT Governance, Privacy and Security Issues*. European Research Cluster on the Internet of Things, January, 2015

Barrett, Zhang, Davies & Barrett (2015): *Clever Classrooms, Summary report of the HEAD Project*. Salford 2015.

De Cremer, Nguyen & Simkin (2017): The integrity challenge of the Internet-of-Things (IoT): on understanding its dark side. *Journal of Marketing Management*. Volume 33, 2017 - Issue 1-2: The Internet of Things (IoT) and Marketing: The State of Play, Future Trends and the Implications for Marketing

EU: IoT Privacy, Data Protection, Information Security, Conclusions of the Internet of Things public consultation. http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation

van den Hoven (undated): Fact sheet, Ethics Subgroup IoT – Version 4.0.

Mantelero, Thobani, Esposito (2017): *Deliverable 4.1 First Report. Virt-EU: Values and Ethics in Responsible Technical Design in Europe*

Matusek, F (2014): *Selective Privacy Protection for Video Surveillance*. Academic Dissertation, Acta Universitatis Ouliensis, A Scientiae Rerum Naturalium 622. http://jultika.oulu.fi/files/isbn9789526204154.pdf

Tieto (2018): *The Future Classroom Project. Do innovative technologies have the potential to transform presence registration?* Skellefteå kommun och Tieto, 2018

BILAGA 1

JURIDISKA ASPEKTER PÅ IOT I SKOLAN

PM avseende användandet av sensorer och teknologi i utbildningsmiljöer

1. Bakgrund

1.1. RISE Research Institutes of Sweden AB ("Rise") deltar i ett projekt som handlar om att på olika sätt använda sensorer och teknologi i utbildningsmiljöer för att kunna förstärka och förbättra undervisningsprocesser.

1.2. Inom ramen för detta arbete har Rise tagit fram ett antal tänkbara framtida scenarion där olika tekniska lösningar som innebär behandling av elevers personuppgifter används. Rise har, i syfte att möjliggöra en diskussion om de konsekvenser som sådana scenarion skulle kunna medföra, och vilka hinder som uppställs i lagstiftningen, ombett oss att lämna våra synpunkter på dem från ett juridiskt perspektiv.

1.3. De tänkta scenariona är följande:

a) En skola vill helt automatisera frånvarohantering genom att kameror i skolan förstår vem som är vem och var de är, och bokför denna information i skolans frånvarosystem.
b) En skola vill samla in data om elevers sömn, rörelse och matvanor för att jämföra dessa med studieresultat och prestation
c) En skola vill samla in data om elevers fysiska rörelse i skolan för att kunna bygga upp modeller över var elever rör sig, upplever trygghet och studiero, för att nyttomaximera skolans lokaler.

Avgränsningar

1.4. Rise har uppdragit oss att övergripande uttala oss om de olika scenarionas förenlighet med vad som stadgas i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG ("Dataskyddsförordningen").

1.5. Inom ramen för detta kortfattade PM har vi utgått från reglerna i Dataskyddsförordningen, lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, skollagen (2010:800) samt kamerabevakningslagen (2018:1200). Annan speciallagstiftning, som skulle kunna bli tillämplig avseende behandling av viss information, exempelvis offentlighets- och sekretesslagen (2009:400), patientdatalagen (2008:355) eller socialtjänstlagen (2001:453) har inte behandlats.

1.6. All rådgivning vi lämnar är anpassad efter uppdraget och utgår från de fakta som presenterats för oss och de instruktioner vi erhåller. Rådgivningen som lämnas av

LEDAMOT AV SVERIGES ADVOKATSAMFUND
Engström & Hellman Advokatbyrå AB
ADRESS: Spannmålsgatan 19
POSTADRESS: 411 05 Göteborg
WEBB: www.engstromhellman.se
E-POST: info@engstromhellman.se
TELEFON: 031-757 99 00
TELEFAX: 031-757 99 01
ORGANISATIONSNR: 556763-8415
STYRELSENS SÄTE: Göteborg

oss är därför inte avsedd att användas i något annat sammanhang än inom ramen för det specifika uppdraget och Rise kan inte förlita sig på rådgivningen utanför uppdragets ram.

1.7. Mot bakgrund av att frågeställningarna till sin natur är sådana att någon detaljerad specifikation av hur den rent faktiska behandlingen av personuppgifter skulle kunna komma att ske inte har lämnats, får de slutsatser som dras i detta PM betraktas som mer allmänt hållna. För det fall Rise eller någon annan aktör skulle vilja gå vidare med implementeringen av någon av de föreslagna funktionerna helt eller delvis behöver frågeställningarna utredas ytterligare.

1.8. Våra allmänna avtalsvillkor gäller för all rådgivning.

2. Övergripande kommentarer

2.1. Samtliga de föreslagna scenariona innebär relativt omfattande övervakningsåtgärder som vidtas mot elever – i vissa fall också underåriga elever. De integritets-skyddsgarantier som uppställs genom Dataskyddsförordningen och annan lagstiftning innebär sannolikt att det i dagsläget skulle vara svårt att implementera sådana åtgärder – i vart fall utan samtycke från vårdnadshavare eller elever. Enligt vår uppfattning krävs därför lagstiftningsändringar – framförallt i skollagen – där skolans uppdrag och ansvar för att samla in data i den omfattning som föreslås, tydliggörs. Huruvida sådan lagstiftning är lämplig eller rimlig ligger inte i vårt uppdrag att uttala oss om.

2.2. Flera av våra resonemang nedan är tillämpliga avseende flera av frågeställningarna. Där vi bedömt att så är fallet hänvisas till tidigare resonemang istället för att upprepa vad som tidigare sagts.

Särskilt om fristående skolor

2.3. De bestämmelser i skollagen och Dataskyddsförordningen samt övriga bestämmelser i refererad lagstiftning som diskuteras gäller som huvudregel på samma sätt för skolor med offentliga huvudmän som för fristående skolor. Det skall emellertid noteras att fristående skolor, till skillnad från skolor med offentliga huvudmän äger rätt att åberopa den rättsliga grunden ”intresseavvägning” i artikel 6.1.f i Dataskyddsförordningen. Mot bakgrund av att de uppgifter som skall behandlas i stor utsträckning är så kallade känsliga uppgifter saknar detta dock i stort betydelse.

Konsekvensbedömning och samråd

2.4. Övergripande får också sägas att den tänkta personuppgiftsbehandlingen i samtliga frågeställningar är sådan att en konsekvensbedömning avseende dataskydd sannolikt behöver genomföras. Enligt artikel 35.1 i Dataskyddsförordningen skall en sådan bedömning göras om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter.

2.5. Så är fallet när det rör sig om systematisk och omfattande bedömning av fysiska personers personliga aspekter som grundar sig på automatisk behandling, och på vilken beslut grundar sig som har rättsliga följder för fysiska personer eller på

liknande sätt i betydande grad påverkar fysiska personer eller när behandling sker i stor omfattning av känsliga uppgifter, se artikel 35.2 i Dataskyddsförordningen.

2.6. Sannolikt skulle den skola som vill påbörja övervakning i större skala med användandet av någon av de föreslagna metoderna också behöva initiera ett förhandssamråd med Datainspektionen med hänvisning till artikel 36 i Dataskyddsförordningen.

3. Automatiserad frånvarohantering

Inledning

3.1. Vi har uppfattat frågeställningen på så vis att en skola, genom att använda kameror eller andra sensorer skall övervaka var varje enskild elev befinner sig under skoldagen och därefter notera eventuella avvikelser i skolans frånvarohanteringssystem. Behandlingen skall vara automatiserad.

3.2. En förutsättning för att frånvarohanteringen skall kunna vara automatiserad, såvitt vi uppfattat frågeställningen, är att biometrisk data om eleverna behandlas i syfte att kunna identifiera dem, på så vis att respektive elevs individuella biometriska uppgifter lagras på förhand och därefter automatiskt jämförs med vad som registreras av kameror eller andra sensorer.

3.3. Den registrerade information används därefter för rapportering av frånvaro till hemmet och till andra eventuella utomstående intressenter, exempelvis Centrala Studiestödsnämnden.

Skollagens reglering av frånvaro

3.4. Enligt 7 kap. 17 § skollagen gäller att om en elev i förskoleklassen, grundskolan, grundsärskolan, specialskolan eller sameskolan utan giltigt skäl uteblir från den obligatoriska verksamheten, skall rektorn se till att elevens vårdnadshavare samma dag informeras om att eleven har varit frånvarande. Om det finns särskilda skäl behöver elevens vårdnadshavare inte informeras samma dag. Såvitt gäller gymnasieskolan har motsvarande bestämmelse intagits i 15 kap. 16 § 2 st. skollagen.

3.5. Mot bakgrund av ovanstående bestämmelser måste en skola behandla uppgifter om en elevs frånvaro för att uppfylla kraven i lagstiftningen. Behandling av uppgifter om frånvaron, som i sig utgör personuppgifter, är således tillåten då behandlingen är nödvändig för att skolhuvudmannen skall kunna fullgöra en rättslig förpliktelse, se artikel 6.1.c i Dataskyddsförordningen. Behandlingen är också tillåten med stöd av artikel 6.1.e i Dataskyddsförordningen eftersom behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i skolans myndighetsutövning.

3.6. Av 7 kap. 19a § skollagen framgår vidare att om en elev i någon av de obligatoriska skolformerna har upprepad eller längre frånvaro från skolverksamheten skall rektorn, oavsett om det är fråga om giltig eller ogiltig frånvaro, se till att frånvaron skyndsamt utreds om det inte är obehövligt. Utredningen ska genomföras i samråd med eleven och elevens vårdnadshavare samt med elevhälsan. En motsvarande bestämmelse för gymnasieskolan återfinns i 15 kap. 16 § 3 st.

3.7. Av bestämmelserna kan utläsas att skolan i vissa fall har en mer omfattande utredningsskyldighet såvitt avser en elevs frånvaro. Av bestämmelsens lydelse står

det dock klart att en sådan utredning normalt är påkallad först efter att det kunnat konstateras att upprepad eller längre frånvaro faktiskt föreligger.

Är behandlingen nödvändig?

3.8. En förutsättning för att behandlingen av personuppgifter i skolans verksamhet skall vara laglig är att den är nödvändig – antingen för att fullgöra en rättslig förpliktelse eller för att utföra en uppgift av allmänt intresse. Detta innebär i princip att personuppgifter bör behandlas endast om syftet med behandlingen inte rimligen kan uppnås genom andra medel, se skäl 39 till Dataskyddsförordningen. Motsatsvis innebär detta att behandling av personuppgifter som är onödigt omfattande mot bakgrund av det syfte som behandlingen sker för, inte är tillåten.

3.9. Var den exakta gränsen går för hur omfattande uppgifter som en skolhuvudman får behandla i syfte att kunna uppfylla sina rättsliga förpliktelser att övervaka och följa upp frånvaro enligt skollagen är inte möjligt att svara på. De mycket korta tidsfristerna som innebär att information om frånvaro skall lämnas till vårdnadshavare samma dag som frånvaron inträffat kräver att skolan tillämpar relativt sofistikerade rutiner för frånvarorapportering. Detta talar för att automatisk behandling av frånvarouppgifter skulle kunna anses nödvändig.

3.10. Det är däremot mer tveksamt om det kan anses som nödvändigt för att uppfylla kraven på frånvarokontroll, att bevaka elevers rörelse under skoldagen eller att kunna följa upp vilka platser de vistats på. Frågan om frånvaro är mer binär på så vis att en elev antingen är frånvarande eller närvarande. Lagstiftningen uppställer inga mellanlägen som gör det relevant att från ett frånvarokontrollsperspektiv inhämta mer uppgifter om exakt var en elev befinner sig.

3.11. Den skyldighet att utreda orsaker till frånvaro som stipuleras i skollagen skall vidare endast göras efter att frånvaro konstaterats och inte i förväg och kan därför inte åberopas som stöd för en mer omfattande frånvarobevakning av samtliga elever.

Behandlingen avser särskilda kategorier av personuppgifter

3.12. Biometriska data som behandlas för att entydigt identifiera en fysisk person tillhör de särskilda kategorier av uppgifter som omfattas av artikel 9 i Dataskyddsförordningen. Behandling av sådana uppgifter är som huvudregel förbjuden, se artikel 9.1. Automatiserad behandling som består i att de övervakade identifieras biometriskt träffas av förbudet i bestämmelsen.

3.13. Flera undantag finns emellertid till förbudet. Av relevans i detta sammanhang är möjligheten att behandla uppgifterna med ett uttryckligt samtycke till behandlingen från den berörde, i detta fall eleven, se artikel 9.2.a i Dataskyddsförordningen. Det är också tillåtet att behandla personuppgifter om behandlingen är nödvändig för ett viktigt allmänt intresse på grundval av nationell lagstiftning, se artikel 9.2.g (observera att till skillnad från vad som anges i artikel 6.1.g i Dataskyddsförordningen används här termen ”viktigt allmänt intresse” istället för endast ”allmänt intresse”).

3.14. I skollagen har intagits en bestämmelse med sådan innebörd som avses i artikel 9.2.g i Dataskyddsförordningen, se 26a kap. 4. § skollagen, där det anges att känsliga personuppgifter, inklusive biometriska uppgifter, får behandlas om behandlingen är

nödvändig för en hantering som motsvarar handläggning av ett ärende hos en myndighet, eller i annat fall, om behandlingen är nödvändig i verksamheten och inte innebär ett otillbörligt intrång i den registrerades personliga integritet.

3.15. Av förarbetena till bestämmelsen framgår att kravet på att behandlingen skall vara nödvändigt bland annat innebär att bara sådana uppgifter som behövs i ärendet eller för den motsvarande hanteringen får behandlas. Begreppet ”nödvändig” innebär emellertid i detta fall inte ett krav på att behandlingsåtgärden skall vara helt oundgänglig. Behandlingen kan anses nödvändig och därmed tillåten om den leder till effektivitetsvinster (se prop. 2017/18:218 s. 218).

3.16. Bestämmelsen är enligt förarbetena dock inte avsedd att tillämpas slentrianmässigt i den löpande verksamheten. Istället krävs att skolhuvudmannen innan behandlingen påbörjas gör en bedömning av om denna innebär ett otillbörligt intrång i elevens personliga integritet. Om behandlingen skulle innebära ett sådant intrång, får den inte ske enligt bestämmelsen. För att avgöra om intrånget är otillbörligt måste skolhuvudmannen göra en proportionalitetsbedömning där behovet av att utföra behandlingen vägs mot elevens intresse av att behandlingen inte sker.

3.17. Bedömningen av elevens intresse av att behandlingen inte sker bör utgå från det intresse av integritetsskydd som denne typiskt sett har. Skolhuvudmannen måste därför enligt förarbetsuttalandet således inte göra en bedömning i förhållande till varje berörd individ utan kan istället göra en övergripande bedömning. Vid bedömningen av intrånget i elevernas personliga integritet skall vikt läggas bland annat vid uppgifternas känslighet, behandlingens karaktär, den inställning eleverna kan antas ha till behandlingen, den spridning uppgifterna kan komma att få och risken för vidarebehandling för andra ändamål än insamlingsändamålet.

3.18. Det skall också nämnas att frågan om användningen av biometrisk data i identifikationssyfte i skolan prövades av regeringsrätten i RÅ 2008 ref. 83. I rättsfallet som rörde identifiering med fingeravtryck för att kunna äta mat i skolmatsalen kom regeringsrätten till slutsatsen att behandlingen var så integritetskänslig att samtycke krävdes från eleven för att åtgärden skulle vara tillåten enligt dåvarande personuppgiftslagen. Vid tidpunkten fanns inte någon skrivning i skollagen motsvarande den som nu införts i 26a kap. och personuppgiftslagen saknade också särskilda bestämmelser om biometriska uppgifter. Slutsatserna i rättsfallet får därför i någon mån anses ha spelat ut sin roll.

3.19. Det går sammanfattningsvis inte entydigt att uttala sig om rörande huruvida den hypotetiska behandlingen av biometriska data i identifikationssyfte är tillåten eller inte mot bakgrund av skollagens utformning. Istället måste en mer omfattande utredning göras av hur den eventuella tekniska lösningen skulle fungera, hur identifieringen rent faktiskt skulle gå till och vilken omfattning personuppgiftsbehandlingen skulle komma att ha.

Förekomst av automatiserat beslutsfattande

3.20. Studiebidrag ges, precis som inackorderingstillägg och extra tillägg, i normalfallet endast för heltidsstudier och de olika typerna av stöd kan dras in om den studerande är frånvarande utan giltigt skäl.

3.21. Skolorna skall rapportera ogiltig frånvaro till Centrala Studiestödsnämnden som sedan kan besluta att dra in studiehjälpen under frånvaron. Sedan den 1 januari 2012 är riktlinjen att skolorna skall rapportera till Centrala Studiestödsnämnden om en studerande är frånvarande utan giltigt skäl mer än några enstaka timmar per månad och om frånvaron är återkommande.

3.22. Skolan skulle alltså mot bakgrund av detta vara skyldig att anmäla resultatet av den automatiserade frånvarohanteringen till Centrala Studiestödsnämnden i de fall villkoren för rapporteringen är uppfyllda, vilket i förlängningen skulle kunna få till konsekvens att en frånvarande elevs studiebidrag dras in.

3.23. Av artikel 22 i Dataskyddsförordningen framgår att en registrerad skall ha rätt att slippa bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne.

3.24. Enligt vår bedömning kan frånvarorapportering som sker med stöd av de automatiskt insamlade uppgifterna om frånvaro kunna utgöra sådant automatiserat individuellt beslutsfattande med rättsliga följder som avses i artikel 22. Sådana åtgärder är som huvudregel förbjudna, se artikel 22.1.

3.25. I vissa fall kan sådant beslutsfattande emellertid vara tillåtet. Så är fallet, såvitt är relevant här, antingen om behandlingen tillåts enligt EU-rätten eller nationell rätt och som fastställer lämpliga åtgärder till skydd för den registrerades rättigheter, friheter och berättigade intressen, eller om behandlingen grundar sig på den registrerades uttryckliga samtycke. Det sistnämnda samtycket behöver då lämnas *utöver* det uttryckliga samtycke som också eventuellt inhämtats för behandlingen av elevens biometriska data (se även artikel 22.4 som vid sådana omständigheter också kräver att lämpliga åtgärder för att skydda den registrerades berättigade intressen har vidtagits). Det skall vidare noteras att det för närvarande, såvitt vi kan se, saknas EU-rättslig eller svensk lagstiftning som skulle medföra någon rätt att använda automatiskt beslutsfattande med rättsliga följder såvitt gäller frånvarohantering.

3.26. Skulle skolan, före rapportering till Centrala Studiestödsnämnden, utföra manuella kontroller av den insamlade datan för att säkerställa att den automatiskt fastställda frånvaronivån hos en viss elev överensstämmer med verkligheten träffas emellertid behandlingen sannolikt inte av förbudet i artikel 22 i Dataskyddsförordningen eftersom ett beslut om att dra in studiestöd då inte enbart skulle grunda sig på automatiserad behandling.

Kamerabevakningslagen

3.27. En skolas möjlighet att använda sig av kamerabevakning regleras, vid sidan om Dataskyddsförordningen av kamerabevakningslagen (2018:1200). Som huvudregel gäller enligt 7§ i lagen att en skola behöver tillstånd för att kamerabevaka den del av ett skolområde eller en skolbyggnad dit allmänheten har tillträde exempelvis skolgårdar och parkeringsplatser. Någon motsvarande skyldighet för att kamerabevaka andra delar av skolområdet dit endast skolpersonal och elever har tillträde uppställs inte i lagen. Kamerabevakning som sker i skolans lokaler kan som huvudregel således ske utan tillstånd. Detta gäller även fristående skolor.

3.28. Oavsett huruvida tillstånd krävs gäller enligt 15 § kamerabevakningslagen att upplysning om kamerabevakning sker skall lämnas genom tydlig skyltning eller på något annat verksamt sätt, samt att om ljud kan avlyssnas eller tas upp vid bevakningen, skall en särskild upplysning lämnas om detta.

3.29. De övriga regler rörande behandling av personuppgifter som gäller enligt Dataskyddsförordningen gäller i övrigt också kamerabevakning. Då kamerabevakning ofta uppfattas som integritetskränkande krävs att skolan beaktar elevernas integritetsintresse på ett sådant sätt att bevakningen inte sker i större omfattning än vad som är nödvändigt mot bakgrund av syftet med bevakningen.

3.30. I detta sammanhang bör skolan bland annat utvärdera och ta ställning till hur många kameror som används, i vilka utrymmen kamerorna är placerade (och därvid undvika övervakning i utrymmen som är särskilt integritetskänsliga såsom toaletter och omklädningsrum), under vilken tid kamerorna är aktiverade, vilken typ av kameror det rör sig om – med fast optik eller möjlighet till inzoomning och huruvida ljudupptagning sker (vilket normalt innebär ett större integritetsintrång).

3.31. Den som övervakas med kamera tillerkänns genom Dataskyddsförordningen en rätt till tillgång till uppgifterna som behandlas. Av förarbetena till kamerabevakningslagen (se SOU 2017:55 s. 342 ff. och artikel 15 i Dataskyddsförordningen) framgår att rätten till tillgång är större om det inspelade materialet är strukturerat på så vis att enskilda personer i bildupptagningen har namn- eller personnummersatts. Vid bildupptagning där biometriska uppgifter används för identifiering torde en sådan rätt därför aktualiseras.

3.32. Slutligen skall anmärkas att Datainspektionens uppfattning är att kamerabevakning inte bör vidtas som en första eller enda åtgärd för att uppnå bevakningssyftet. Istället bör det alltid övervägas om målet med bevakningen kan uppnås på annat sätt, exempelvis genom att utöka personalen eller vidta andra åtgärder. Såvitt gäller frånvarokontroll kan sådan fortsatt lätt göras genom upprop i klassrummet, vilket talar mot användning av kamerabevakning för detta syfte.

Rättssäkerhet i myndighetsutövningen

3.33. Som framgår ovan kan skolan i många fall komma att använda den information som framkommer genom ett system för automatiskt frånvarohantering på ett sätt som påverkar den enskilda elever. Det kan röra sig om rapportering till Centrala Studiestödsnämnden, rapportering till vårdnadshavare med stöd av 7 kap. 17 § skollagen, vidtagande av frånvaroutredning med stöd av 7 kap. 19a § skollagen samt i vissa fall i samband med disciplinära åtgärder. Flera av dessa åtgärder är att betrakta som myndighetsutövning.

3.34. Som en allmänt vedertagen förvaltningsrättslig princip gäller att beslut som fattats vid myndighetsutövning skall kunna motiveras, att besluten skall ha stöd i lag och att den som är part i ett ärende skall beredas insyn i beslutsprocessen. I vissa fall kan beslut som rör enskilda också överprövas i domstol. För att i efterhand kunna fastställa om ett beslut tillkommit i laga ordning och om det är materiellt korrekt krävs att det underlag som ligger till grund för beslutet kan granskas och förklaras.

3.35. Vid automatisk identifiering av elever kan ett stort antal felkällor vara för handen. Den algoritm som ligger till grund för jämförelsen mellan de biometriska uppgifter som registreras av sensorer och kameror och de lagrade biometriska uppgifterna rörande respektive elev, kan vara behäftad med fel som gör att personers identitet förväxlas eller att en elev inte alls korrekt identifieras på grund av förekomsten av exempelvis en keps eller en huvudduk som skymmer ansiktet. Resultatet av sådana misstag skulle kunna bli att en viss åtgärd som riktas mot en viss elev blir felaktig.

3.36. Beroende på hur tydligt och fullständigt det underlag som legat till grund för den felaktiga identifieringen har varit kan det i efterhand visa sig bli svårt att rent faktiskt sluta sig till hur det automatiserade systemet har kommit till en viss slutsats vilket skulle göra det vanskligt att kontrollera riktigheten i informationen.

3.37. Eftersom många beslut som fattas med stöd av skollagen inte går att överklaga ställer detta naturligtvis höga krav på den enskilde beslutsfattaren. Detta talar enligt vår mening för att höga krav måste ställas på de uppgifter som registreras så att resultatet av behandlingen blir begripligt för elever och vårdnadshavare. Uppgifter som ligger till grund för någon åtgärd mot en enskild elev måste också sparas, i vart fall under så lång tid att ett överklagande eller en begäran om omprövning av ett beslut på ett meningsfullt sätt kan prövas och granskas.

Uppgifter om andra än elever

3.38. Ett särskilt problem som kan uppstå vid övervakning av elever med kameror i skolan är att även skolpersonal och andra personer som vistas i skolan kan komma att inkluderas i bild- och ljudupptagning. Genom detta kan deras biometriska personuppgifter komma att behandlas trots att dessa personers närvaro inte är det som är syftet med övervakningen. Även denna behandling är sannolikt att bedöma som en behandling av sådana känsliga uppgifter som avses i artikel 9.1 i Dataskyddsförordningen.

3.39. Den särskilda bestämmelse som införts i 26a kap. 4 § skollagen och som tillåter behandling av känsliga uppgifter är dock inte begränsad till behandling av uppgifter om elever. Mot denna bakgrund kan behandlingen av biometriska uppgifter om andra än elever i vissa fall vara tillåten, dock under förutsättning att uppgifterna endast används för det uppgivna syftet, nämligen att övervaka elevernas – och inte exempelvis medarbetarnas – närvaro. Det skall dock noteras att införandet kamerabevakning normalt utlöser en förhandlingsskyldighet enligt medbestämmandelagen, se 21 § kamerabevakningslagen.

4. Insamling av data om elevers sömn, rörelse och matvanor

Inledning

4.1. Vi har uppfattat frågeställningen på så sätt att en skola genom sensorer eller någon annan teknisk lösning skulle registrera elevers beteenden under hela dygnet i syfte att kunna dra slutsatser på individuell nivå om hur olika typer av beteenden eller beteendeförändringar påverkar elevens studieresultat och prestationer. En förutsättning för datainsamlingen kan därmed vara att eleven bär någon form av teknisk hårdvara på kroppen i syfte att mäta exempelvis puls, andning, gånghastighet och GPS-position.

Ligger datainsamlingen inom skolans kompetensområde

4.2. Visserligen framgår i 4 kap. 3 § skollagen att varje huvudman inom skolväsendet på huvudmannanivå systematiskt och kontinuerligt skall planera, följa upp och utveckla utbildningen. Det får dock ifrågasättas om denna typ av detaljerade studier av elevernas beteenden utanför skoltid ryms inom ramen för detta uppdrag, eller inom ramen för skolans uppdrag överhuvudtaget – trots att den information dylika studier skulle kunna generera möjligen skulle ge lärare och skolpersonal värdefull kunskap som i slutändan skulle kunna vara till gagn för elevens utveckling.

4.3. Det ligger däremot mer nära till hands att en skola inom ramen för sin verksamhet under skoltid samlar in data om eleverna i syfte att stimulera elevernas utveckling mot kunskapsmålen. En avgörande fråga i sammanhanget är därför vad som utgör skoltid och vad som inte gör det.

4.4. Det finns ingen generell definition av begreppet skoltid som går att använda i alla situationer. I ett beslut från Skolverket (beslut med dnr. 51-2006:2850 av den 31 januari 2007) har den tid då tillsynsansvaret går över på skolan, vilket kan betraktas som vägledande för skoltidsbegreppet, definierats som den tid då ett barn befinner sig i skolan eller fritidshemmet. I doktrin har begreppet vidgats något och har där bland annat definierats som den tid då eleven befinner sig i skolan eller deltar i annan av skolan annorstädes anordnad verksamhet, med utgångspunkt tagen i den schemalagda eller på annat sätt bestämda undervisningstiden och en viss, kortare, tid före och efter skoldagens slut (se härvid Engström & Hellman, Ungdomars fri- och rättigheter i föreningsliv och skola, s. 135 f.)

4.5. Insamling av data om elevernas beteende som sker utanför skoltid skulle enligt vår uppfattning ske helt utanför det skollagsreglerade området, trots att skolan i viss omfattning har skyldighet att vidta hälsofrämjande insatser inom ramen för elevhälsan (se vidare nedan). Skolpersonal har i och för sig vissa skyldigheter att uppmärksamma och anmäla missförhållanden som en elev kan utsättas för i hemmet (se 14 kap. 1 § socialtjänstlagen som också gäller fristående skolor), men lagstiftningen ställer inget krav på skolpersonalen att vidta några omfattande utredningar om elevens hemmiljö. Sådana utredningsåtgärder får istället vidtas av socialtjänsten.

4.6. Skolan har således varken rätt eller skyldighet inom ramen för dagens lagstiftning att övervaka exempelvis elevers mat- eller sömnvanor eller rörelsemönster även om sådana uppgifter naturligtvis kan ha viss betydelse för studieresultat och möjlighet att ta till sig själva utbildningen. En eventuell kartläggning av elevers sömn, rörelse och kosthållning måste därför ske med stöd av frivillighet från elevers och vårdnadshavares sida i den mån den sker utanför skoltid.

4.7. Sker uppgiftsinsamlandet under skoltid gör sig i princip samma överväganden gällande som gäller avseende automatiserad frånvarokontroll och som behandlats ovan. Det skall dock anmärkas att förekomsten av GPS-positionering eller motsvarande teknik för att bestämma var en elev befinner sig, sannolikt skulle bedömas som ännu mer integritetskränkande än positionering genom kamerabevakning.

4.8. För det fall datainsamligen kräver särskild hårdvara, exempelvis genom att eleven behöver använda ett aktivitetsarmband, en ”smart klocka” eller någon annan likande hårdvara som krävs för insamlingen, krävs naturligtvis också att eleven eller vårdnadshavaren samtycker till detta.

Uppgifter om hälsa

4.9. Uppgifter om en fysisk persons hälsa tillhör de särskilda kategorier av uppgifter som omfattas av artikel 9 i Dataskyddsförordningen. Behandling av sådana uppgifter är, liksom biometriska uppgifter för entydig identifiering, som huvudregel är förbjuden.

4.10. Hälsouppgifter utgör enligt Dataskyddsförordningen alla de uppgifter som hänför sig till en registrerad persons hälsotillstånd som ger information om den registrerades tidigare, nuvarande eller framtida fysiska eller psykiska hälsotillstånd. Detta inbegriper bland annat uppgifter om den registrerades fysiologiska eller biomedicinska tillstånd, oberoende av källan, exempelvis från en läkare eller en medicinteknisk produkt, se skäl 35 till Dataskyddsförordningen Detta innebär att uppgifter om exempelvis sömn, kost och rörelse kan utgöra hälsouppgifter.

4.11. Enligt 2 kap. 25 § skollagen skall det för såväl de obligatoriska skolformerna som för gymnasieskolan finnas elevhälsa. Elevhälsan skall omfatta medicinska, psykologiska, psykosociala och specialpedagogiska insatser och skall främst vara förebyggande och hälsofrämjande. Av bestämmelsen framgår också att elevernas utveckling mot utbildningens mål ska stödjas.

4.12. En skola äger rätt att behandla uppgifter om elevernas hälsa inom ramen för elevhälsan. Den personuppgiftsbehandling som sker inom ramen för elevhälsans medicinska verksamhet omfattas dock av patientdatalagens bestämmelser. Övrig behandling av känsliga personuppgifter inom ramen för skolans hälsofrämjande uppdrag sker med stöd av 26a kap. skollagen som berörts närmare ovan. Skolan får således i och för sig behandla uppgifter om exempelvis elevers kosthållning, sömnvanor och fysiska aktivitet i den mån uppgifterna är relevanta för att bedöma elevens hälsotillstånd eller för att arbeta hälsofrämjande.

Underårigas möjlighet att lämna samtycke

4.13. En särskild fråga vid inhämtande av samtycke från skolelever är vid vilken ålder en underårig själv kan lämna ett samtycke till behandlingen.

4.14. Dataskyddsförordningen uppställer inte någon tydlig åldersgräns för samtycke, men förordningens krav på att samtycken skall vara såväl frivilliga som specifika, informerade och otvetydiga (se skäl 32 i Dataskyddsförordningen) innebär sannolikt att barn i många fall inte kan lämna samtycken på grund av bristande mognad.

4.15. Enligt artikel 8 i Dataskyddsförordningen gäller, såvitt avser informationssamhällets tjänster (exempelvis sociala medier) att medlemsstaterna i nationell rätt kan föreskriva att barn skall kunna samtycka till personuppgiftsbehandling från 13 års ålder. En sådan bestämmelse har också införts i 2 kap. 4 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. Eftersom det således är möjligt för den som är 13 år eller äldre att samtycka till exempelvis Facebooks eller Instagrams mycket komplexa personuppgiftsbehandling ligger det nära till hands att anta att en 13-åring också skulle kunna samtycka till mindre komplex

behandling av hälsodata inom ramen för skolans verksamhet. Det är emellertid inte möjligt att med säkerhet uttala sig om detta utan att först mer noggrant analysera den tänkta personuppgiftsbehandlingen.

4.16. Om barnet inte har uppnått tillräcklig ålder måste samtycke till behandlingen inhämtas från den som har föräldraansvaret för barnet, i normalfallet barnets vårdnadshavare.

Koppling till betygsättning m.m.

4.17. Det skall slutligen särskilt betonas att de eventuella slutsatser som en skolhuvudman kan komma att dra om elevers beteenden såvitt avser mat, sömn och rörelse i normalfallet överhuvudtaget inte får kopplas till betygsättning av eleven. Det förefaller också direkt olämpligt att uppgifterna används vid bedömning av huruvida disciplinära åtgärder skall vidtas mot en enskild elev.

4.18. Om förutsättningen för det lämnade samtycket är att uppgifterna som samlas in endast skall användas för att kunna utvärdera elevens prestationer och studieresultat och för att kunna erbjuda elever verktyg för att bättre kunna ta till sig undervisningen får uppgifterna endast användas för detta syfte.

5. Insamling av data om elevers fysiska rörelse i skolan

Inledning

5.1. Frågeställningen gäller såvitt vi uppfattat möjligheten att registrera elevers rörelsemönster och att därefter använda dessa data för att förbättra den fysiska och psykosociala skolmiljön.

5.2. Även om föremålet för behandlingen av uppgifter i detta fall i viss mån skiljer sig åt från de frågeställningar som diskuterats i samband med scenariot som rör automatisk frånvarohantering, förefaller de metoder som används rent tekniskt för att behandla personuppgifter vara likartade med vad som där gör sig gällande. Detta innebär också att merparten av vad som inom ramen för det scenariot diskuteras rörande kamerabevakning, förekomsten av känsliga uppgifter samt integritetsaspekter är detsamma också avseende detta scenario.

Skolhuvudmännens skyldigheter att skapa trygghet och studiero

5.3. Enligt 5 kap. 3 § skollagen gäller att utbildningen skall utformas på ett sådant sätt att alla elever tillförsäkras en skolmiljö som präglas av trygghet och studiero. Skolhuvudmännen har därutöver också enligt 6 kap. skollagen långtgående skyldigheter att förebygga och förhindra kränkande behandling i skolan och skall också bedriva ett målinriktat arbete för att motverka sådana kränkningar. Även arbetsmiljölagens bestämmelser ställer krav på skolhuvudmännen att utforma den fysiska och psykosociala arbetsmiljön på ett godtagbart sätt.

5.4. Inom ramen för dessa skyldigheter ligger naturligtvis såväl ett aktivt tillsynsansvar såvitt gäller mindre barn och i viss mån en skyldighet att övervaka elevernas beteenden gentemot varandra under lektionstid och på raster. Det är enligt vår uppfattning tveksamt om exempelvis rastvakter skulle kunna ersättas av övervakning som sker med hjälp av tekniska lösningar. Sådana lösningar får därför

ses som ett komplement till, och inte ersättning för, övriga åtgärder som en skola vidtar för att skapa trygghet och motverka kränkningar.

Teknikval har betydelse

5.5. Beroende på vilken teknik som används för att fastställa elevers rörelsemönster kan den integritetskränkning som insamlingen och behandlingen av uppgifter innebär vara större eller mindre. Om informationen exempelvis samlas in genom exempelvis rörelsedetektorer, som utan att det är möjligt att identifiera någon enskild person skapar ett anonymiserat underlag är det inte ens självklart att behandlingen alls skall betraktas som en behandling av personuppgifter och Dataskyddsförordningen är då inte tillämplig.

5.6. Samlas datan däremot istället in genom att ett flertal kameror monteras som gör det möjligt att följa enskilda elevers rörelse genom skolbyggnaden eller på skolgården blir naturligtvis integritetskränkningen betydligt större och motsvarar den som föreslagits såvitt gäller frågan om automatisk frånvarohantering.

5.7. Det skulle naturligtvis också vara möjligt att samla in data på samma sätt som diskuteras i frågan rörande insamling av data rörande kosthållning, sömn och motion ovan, nämligen genom att använda någon form av aktivitetsarmband eller liknande med användning av GPS-positionering. Även mätning av puls eller andning skulle kunna användas för att dra slutsatser om tryggheten på vissa platser i och utanför skolbyggnaden. Behandling av detta slag är emellertid, på samma vis som ovan anförts, mycket integritetskänslig och måste enligt vår uppfattning grunda sig på frivillighet och elevens samtycke.

Göteborg, 2018-12-20

ENGSTRÖM & HELLMAN

Fredrik Engström
Advokat

AVSLUTANDE ANMÄRKNINGAR

Utöver vad som framgår i PM:n kan följande anmärkningar göras i denna del:

Vad gäller p. 3.3.4 nedan kan det noteras att När det gäller skolor med kommunal huvudman bör man notera ett förslag på lagändringar enligt SOU 2018:25, som har varit på remiss och föreslås träda i kraft den 1 juli 2019. Det är dock oklart om förslaget träder i kraft. Förslaget gäller ändringar i offentlighets- och sekretesslagen (OSL) och är relevant för kommunala huvudmän, eftersom OSL gäller för dem.

Utifrån förslaget kan det tänkas att lagändringen ger insyn i myndigheternas verksamhet när algoritmer eller datorprogram används vid vissa automatiserade förfaranden, till exempel när algoritmer används för att få fram underlag till ett individuellt beslutsfattande (automatiserat individuellt beslutsfattande).

Enligt förslaget skulle 4 kap. 3 § offentlighets- och sekretesslagen (OSL) ändras, så att handläggande myndigheter (som huvudregel) blir skyldiga att föra eventuellt digitalt beslutsunderlag till handlingarna i målet eller ärendet.

Enligt förslaget skulle 4 kap. 3 § OSL se ut såhär efter lagändringen:

> *”Om en myndighet för handläggning av ett mål eller ärende använder sig av ett underlag i en databas eller annan digital källa, ska underlaget tillföras handlingarna i målet eller ärendet i läsbar form. En myndighet behöver inte tillföra underlaget till handlingarna i målet eller ärendet enligt första meningen om det finns särskilda skäl mot det.*
>
> *När en myndighet tillämpar första stycket andra meningen ska myndigheten se till att information kan lämnas om vilken eller vilka databaser eller andra digitala källor som innehåller ett underlag för handläggningen av målet eller ärendet.”*

Det är visserligen osäkert om lagförslaget ovan påverkar den aktuella frågan, eftersom lagändringen (än så länge) inte är beslutad. Men det finns ändå anledning att bevaka frågan, eftersom det skulle påverka kommunala huvudmäns hantering av digitalt beslutsunderlag (t.ex. om underlaget är AI-genererat).

Vad gäller p. 3.3.6 nedan kan det för det första noteras att det hör till saken att svårigheterna att “kontrollera riktigheten i informationen” beror helt på vilken insyn som skolhuvudmännen har i det automatiserade systemet. Det är därför tänkbart att skolhuvudmännen – trots utmaningarna – säkerställer insyn i AI-genererat beslutsunderlag och därmed motverkar problemet. Det kan t.ex. ske genom regelbundna kvalitetskontroller som genomförs av personuppgifts-ansvarig. Se SOU 2018:25 sid. 139 med där gjorda hänvisningar till Se artikel 29-gruppens vägledning (”Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17 EN WP 251, Adopted on 3 October 2017”, sid. 9 f.) om beslut som enbart grundas på automatiserad behandling.

Där betonas också att ”personuppgiftsansvariga kan utforska möjligheter till certifieringsmekanismer eller uppförandekoder för tillsyn av processer som involverar maskininlärning, liksom översyn av etiska kommittéer eller liknande för att värdera risker och nytta med den profilering som avses.”

Vad gäller p. 3.3.6 nedan kan det för det andra noteras att liknande frågor tas upp i Europarådets riktlinjer av den 25 januari 2019 om artificiell intelligens och dataskydd (https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8). Riktlinjerna är inte bindande, men kan vara intressanta från ett juridiskt perspektiv i frågor som rör AI inför beslutsfattande. En intressant fråga som betonas i riktlinjerna är bland annat vikten av att upphandlande myndigheter ska ställa krav på tjänsteleverantörers och utvecklares personuppgiftsbehandling i AI-relaterade frågor. Jag tänker mig att det t.ex. kan vara intressant i de fall där algoritmer används vid datainsamling inför beslut enligt skollagen. I framtiden kan det därför vara intressant att bevaka om – och i så fall i vilken utsträckning – riktlinjerna efterlevs vid offentlig upphandling för kommunala skolhuvudmän.

Vad gäller p. 4.5 nedan så kan slutsatsen att ”insamling av data om elevernas beteende som sker utanför skoltid skulle ... ske helt utanför det skollagsreglerade området”, diskuteras. Enligt förarbetena till skollagen (prop 2005/06:38 s. 142) kan ju huvudmannens ansvar att motverka kränkande behandling enligt 6 kap. skollagen även gälla sådana händelser som sker utanför skoltid om de har ett nära samband med verksamheten. I Skolinspektionens praxis har skolan därför t.ex. varit skyldiga att motverka nätmobbing som skett utanför skoltid (se bland annat Skolinspektionens beslut den 13 februari 2017, dnr 41-2016:5708). Med den utgångspunkten kan man därför tänka sig att insamling av personuppgifter om elevers beteende utanför skoltid ändå kan ses som relevant för skolhuvudmannens skyldigheter att motverka kränkande behandling enligt 6 kap. 10 § skollagen. Att personuppgiftsbehandlingen i så fall måste ske enligt GDPR är en annan sak.

PROJEKTPARTNERS

	Kungsbacka	RI.SE Research Institutes of Sweden
ATEA	Eskilstuna kommun	FALKÖPING KOMMUNEN
INTERNET OF THINGS SVERIGE	LIDINGÖ STAD	Microsoft
NTI GYMNASIET	:rytmus MAKE | MUSIC | LIVE	Skellefteå kommun
Stadsmissionens Skolstiftelse	Stockholms universitet	VÄSTERVIKS KOMMUN