Rapport- Executive Order 12333, Presidential Policy Directive 28, Executive Order 14086

Hvordan bruke dette dokumentet?

Dette dokumentet er en vurdering av om det er grunn til å tro at EO 12333 får anvendelse på en kommunes behandling av personopplysninger i Google Workspace for Education.

Dette dokumentet kan være en del av din Transfer Impact Assessment / tredjelandsvurdering hvis du bruker EUs Standard Contractual Clauses (SCC) som overføringsgrunnlag for personopplysninger til USA når du bruker systemer som tilsvarer Google Workspace for Education.

Denne vurderingen kan også brukes som en del av en tredjelandsvurdering hvis adekvansvurderingen blir ugyldiggjort og du som bruker Google Workspace for Education på nytt må bruke SCC som overføringsgrunnlag.

NB: Hvis adekvansvurderingen blir ugyldiggjort, kan det være at EO 14086 ikke lenger gjelder, og da må denne vurderingen justeres før du kan bruke den!

1. INNLEDNING

1.0. Overordnet problemstilling

Er det grunn til å tro, på bakgrunn av lovtekst/teori og praksis, at personopplysninger fra norske skoler som behandles i Google Workspace for Education, vil være gjenstand for overvåkning etter Executive Order 12333?

1.1. Metode

Denne gjennomgangen er innrettet samme metodiske tilnærming som Sikts «transfer impact assessment».

Sikt er kunnskapssektorens tjenesteleverandør, og deres vurdering av hvorvidt den amerikanske etterretningsloven FISA 702 kommer til anvendelse, er trukket frem som en eksempelsak av Datatilsynet i deres veileder for overføring av personopplysninger ut av EØS.

Datatilsynet har ikke godkjent Sikts vurdering av FISA 702, men bekrefter i veiledningen at det er handlingsrom i personvernregelverket til å vurdere hvordan problematisk lovgivning fungerer i praksis (slik som Sikt har gjort). Videre har Datatilsynet uttalt at Sikts presentasjon i veiledningsmøtet tydet på grundige og metodisk gode vurderinger. Så langt prosjektet er kjent, hadde Datatilsynet ingen innvendinger til hvordan vurderingene var blitt gjennomført.

Sikts metode innebærer en todelt vurderingsmodell der den overordnede problemstillingen vurderes ut fra to ulike utgangspunkter; først en gjennomgang av aktuell lovtekst/teori i tredjelandet, deretter en gjennomgang av tredjelandets praksis på området. På denne måten er ambisjonen å finne ut om det er «grunn til å tro» at den problematiske loven får anvendelse, og at den dermed vil komme i konflikt med GDPR.

1.2. Rettskilder

Executive Order 12333 suppleres av flere tilknyttede regelverk og andre støttedokumenter. Etter Snowden-avsløringene i 2014 ble Presidential Policy Directive 28 (PPD-28) presentert som et supplerende regelverk til EO 12333. EO 14086 ble innført høsten 2022 som en forutsetning for Data Privacy Framework. I tillegg til PPD-28 og EO 14086, finnes også «håndbøker», interne prosedyreskriv («Implementing Procedures») og annet veiledningsmateriell som vil inkluderes i denne gjennomgangen.

Gjennomgangen avgrenses mot de avsnitt og passuser i regelverkene som vurderes som mindre relevant og av mindre betydning for den overordnede problemstillingen.

1.3. Noen forbehold

Executive order 12333 er et omfattende regelverk. Både i antall bestemmelser, men også i mengde ren tekst og supplerende støttemateriell. Videre bærer EO 12333 tydelig preg av å være utformet etter den engelske «common law» - tradisjonen.

«Common Law»-tradisjonen kjennetegnes av prinsippet om «stare decisis», som bl.a. innebærer at gjeldende rett primært utformes etter domstolsavgjørelser og presedens. Lovteksten får på denne

måten en slags underordnet rolle ved tolkning. Innenfor rettskulturer der lovtekst ikke er det primære tolkningssubjektet i en rettsanvendelsesprosess, utfylles lovteksten gjerne med større mengder tekst. Men selv om lovteksten her er utfyllende, blir den samtidig mer tvetydig. Det mangler også klar anvisning på konkrete vurderingstema eller annen veiledning for å tolke og utlede gjeldende rett. På denne måten vil Lovteksten i de fleste amerikanske regelverk undras en tradisjonell norsk rettsanvendelsesprosess. I kombinasjon med en svært uoversiktlig regelstruktur, er det en utfordrende øvelse å utlede noe konkret og substansielt fra lovteksten. Ettersom lovtekst er den eneste rettskildetypen som er tilgjengelig på dette tidspunktet, vil prosjektets mulighet til å konkludere på den overordnede problemstillingen, være noe begrenset.

Denne rapporten inneholder ikke en fullstendig gjennomgang av regelverkene som vurderes. Gjennomgangen konsentreres heller rundt utvalgte deler av hvert enkelt regelverket som, etter prosjektets forståelse, fremstår som relevant. Det er derfor en risiko at gjennomgangen utelater øvrige deler som likevel kan være relevante i lys av den overordnede problemstillingen. Denne rapporten må ikke leses som en komplett lovkommentar.

Forbehold tas i den grad vurderingene i denne rapporten ikke reflekterer korrekt eller fullstendig bruk av amerikanske rettskilder.

2. EXECUTIVE ORDER 12333: UNITED STATES INTELLIGENCE ACTIVITIES

2.0. BAKGRUNN

Det er en kjensgjerning at amerikanske myndigheter bedriver omfattende overvåknings- og etterretningsvirksomhet rettet mot mål utenfor USAs egne grenser. Dokumenter som ble offentliggjort av Edward Snowden i 2014 viser blant annet at «National Security Agency»(NSA) kontinuerlig gjennomfører utenlandske overvåkningsoperasjoner som resulterer i oversending eller lagring av store mengder elektronisk kommunikasjon og personopplysninger.

NSA regnes for å være den ledende amerikanske aktøren innen kryptologi og cybersikkerhetstjenester. NSAs virksomhet inkluderer bl.a. signaletterretning, samt datanettverksoperasjoner. Formålet med virksomheten er å oppnå «[…]a decisiv advantage for the nation and our allies.».[1]

NSAs overvåkningsvirksomhet reguleres primært av Executive Order 12333 (EO 12333).
En «Executive Order», eller presidentordre, er et internt direktiv/ordre som utstedes fra presidenten. Direktivenes formål er å instruere departementene, eller "the executive branch" i deres forvaltningsoppgaver. Presidenten kan når som helst tilbakekalle, endre eller gjøre unntak fra enhver presidentordre, enten ordren ble gitt av den nåværende presidenten eller en forgjenger. Vanligvis gjennomgår en ny president gjeldende ordrer i løpet av de første ukene i embetet. Dette gjør presidentordre sårbare som rettskilde, og det hefter derfor en betydelig risiko knyttet kontinuiteten i disse regelverkene.

2.1. DEFINISJONER

Overvåkning – Samlebetegnelse for innhenting, forvaltning og håndtering av opplysninger, data, og annen informasjon som ikke er offentlig tilgjengelig.

Overvåkningsaktør – Samlebetegnelse for amerikansk statlig aktør som etter EO 12333 har myndighet til å drive overvåkning- og etterretningsvirksomhet.

Overvåkningsaktivitet - Samlebetegnelse for ulike former for overvåkning. Begrepet begrenses i denne vurderingen til overvåkning som faller inn under signaletterretning (SIGINT).

GWE – Tjenester og produkter som Google tilbyr i forbindelse med leveransen av Google Workspace for Education til norske skoler

"Signals intelligence Activities" – En form for overvåkning som baserer seg på aktiv eller passiv oppfanging og innsamling av signaler. Den norske oversettelsen er signaletterretning. Dette kan eksempelvis være dataoverføringer, telekommunikasjon, radiobølger m.m. [2]

[1] https://www.nsa.gov/about/
[2] https://www.etterretningstjenesten.no/om-etterretning/prosess-og-metoder

2.2. «PART 1 - GOALS, DIRECTIONS, DUTIES, AND RESPONSIBILITIES WITH RESPECT TO UNITED STATES INTELLIGENCE EFFORTS»

2.2.1. AKTØRER MED OVERVÅKNINGSMYNDIGHET

I henhold til EO 12333 Section (Sec.) 1.7 t.o.m. Section 1.13 mobiliseres og forpliktes sentrale nasjonale aktører («agencies») til å gjennomføre innsamling, analysering, produksjon og formidling av informasjon til «Director of National Intelligence». Av betydning her er det særlig at samtlige av de nasjonale aktørene – med få unntak, pålegges å gjennomføre nært sagt den samme overvåkningen. Listen av aktører inkluderer blant annet:

- Central Intelligence Agency (CIA),
- Defense Intelligence Agency,
- National Security Agency (NSA),
- National Geospatial-Intelligence Agency, Intelligence And Counterintelligence Elements Of The Army, Navy Air Force, And Marine Corps,
- Federal Bureau Of Investigation (FBI),
- Intelligence And Counterintelligence Elements Of The Coast Guard,
- The Bureau Of Intelligence And Research,
- Department Of State; The Office Of Intelligence And Analysis,
- Department Of The Treasury;
- The Office Of National Security Intelligence,
- Drug Enforcement Administration;
- The Office Of Intelligence And Analysis,
- Department Of Homeland Security;
- The Office Of Intelligence And Counterintelligence,
- Department Of Energy

2.2.2. MÅL FOR OVERVÅKNING

Lovteksten virker ikke å regulere nærmere hvilke mål som er aktuelle å overvåke. Det angis heller ikke hvilke vurderinger som ligger til grunn for utvelgelse av mål. I denne sammenheng beskriver Part 1 kun de overordnede formål med overvåkningene. De overordnede formålene inkluderer bl.a. styrking av sikkerhet, antiterror, kontraetterretning.[3] På denne måten fremstår EO 12333 å være innrettet en slags «alt og ingenting»-tilnærming. Slik sett er det lite i lovteksten som tilsier at data fra norske skoler som bruker GWE vil være gjenstand for overvåkning. Her må det imidlertid merkes at det heller ikke er holdepunkter for å si at data fra norske skoler som bruker GWE *ikke* vil være gjenstand for overvåkning.

I den grad «part 1» kan sies å regulere rammene for innsamling av data, er det ingen holdepunkter i lovteksten som tilsier at Bergen kommunes informasjon vil være gjenstand for særskilt overvåkning. Foruten de forpliktelser som følger av Sec. 1.7 t.o.m. 1.13 (se over), fremstår «part 1» mer som et innledende kapittel der overordnede formål og lignende beskrives.

[3] Se bokstav (d) punkt 1-3

2.2.3. DELKONKLUSJON – PART 1:

Basert på lovteksten i Part 1, kan det ikke utelukkes at personopplysninger om barn vil bli gjenstand for overvåkning ved bruk av GWE i norske skoler.

2.3. «PART 2 - CONDUCT OF INTELLIGENCE ACTIVITIES»

2.3.1. INNHENTING AV «SIGNIFICANT FOREIGN INTELLIGENCE»

Det følger av Sec. 2.2 (s.711) om «Purpose», at «[t]his Order is intended to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, […]».

I den grad Sec.2.2 oppstiller rammer for innhenting av data, blir spørsmålet videre om Bergen kommunes data i Google Workspace for Education kan regnes som «significant foreign intelligence».

Begrepet «Foreign intelligence» defineres nærmere under Sec.3.5 bokstav (e) som «information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.».

Etter ordlyden følger det ingen rimelige begrensninger på verken mengde eller type data som kan samles inn. Selv om lovgiver bruker «significant» for å ramme inn begrepet «foreign intelligence», er det likevel ikke grunnlag for å tolke dette som en vesentlig rettslig terskel.

Hva som kan regnes som «significant» må rimeligvis bestemmes ut fra det formål, interesse eller behov som opprinnelig begrunner innsamlingen. I den forbindelse er det USA og aktørene med overvåkningsmyndighet som i fellesskap definerer dette i henhold til reglene de er underlagt (EO 12333, FISA, Konstitusjonen). Og med utgangspunkt i lovens formål slik det bl.a. er beskrevet i part 1 om styrking av sikkerhet, antiterror, og kontraetterretning, kan disse begrepene neppe tolkes innskrenkende eller strengt all den tid begrepene er så overordnede og på den måten nærmest altomfattende.[4]

Formuleringen i Part 1 Sec. 1.1 bokstav (e) underbygger også denne forståelsen. Her følger at «[s]pecial emphasis shall be given to the production of timely, accurate, and insightful reports, responsive to decisionmakers in the executive branch, that draw on **all appropriate sources of information**, including open source information, meet rigorous analytic standards, consider diverse analytic viewpoints, and accurately represent appropriate alternative views.» (mine uthevninger).

Ordlyden understreker viktigheten av at aktører med overvåkningsmyndighet utnytter alle passende datakilder. Så lenge en bestemt datakilde potensielt kan avgi informasjon egnet til å belyse forhold som kan styrke sikkerheten i USA, er berørte aktører påkrevd å utnytte denne. Når det gjelder rammene for innhenting av data, nevner ikke lovteksten hva som ligger i begrepet «appropriate sources of information». Det kan her stilles spørsmål om lovgiver bevisst har valgt å være upresis. Dette kan i så fall skyldes at tvetydig og upresis ordlyd åpner aktørenes handlingsrom, noe som er i tråd med fullmaktsstrukturen som gjennomgås nærmere i punkt 2.5 og 3.2 under.

Samlet sett er det få holdepunkter i «part 2» som støtter en påstand om at Bergen kommunes informasjon skulle være av særskilt interesse – i alle fall sammenlignet med ethvert annet tilfeldig datasett i enhver annen digital løsning eller tjeneste. Problemet er nok heller at adgangen, omfanget og de generelle overvåkningskapasitetene som nasjonale aktører i USA besitter, nærmest ser ut til å

[4] Se bokstav (d) punkt 1-3)

være ubegrenset. Av særlig betydning her er det at verken lovtekst eller annet supplerende rammeverk i nevneverdig grad begrenser mulighetene til overvåkning etter EO 12333.

2.3.2. DELKONKLUSJON – PART 2:

Basert på lovteksten i Part 2, kan det ikke utelukkes at personopplysninger om barn vil bli gjenstand for overvåkning ved bruk av GWE i norske skoler.

2.4. «PART 3 – GENERAL PROVISIONS»

«Part 3» i EO 12333 inneholder utfyllende og supplerende bestemmelser opp mot de prinsipper, føringer og andre overordnede regler som allerede er etablert i part 1 og 2. Part 3 Sec.3.5 inneholder også en seksjon med begrepsdefinisjoner.

I tråd med prinsippene etablert i «Part 2» om «CONDUCT OF INTELLIGENCE ACTIVITIES», skal hver «agency» som er forpliktet til å gjennomføre overvåkning etter part 1, etablere «appropriate procedures and supplementary directives consistant with this order».

Etter ordlyden opereres det med en slags ansvars- og fullmaktsstruktur hvor aktører som er ustyrt med myndighet til å overvåke, selv velger hvordan de ønsker å imøtekomme prinsippene som er knesatt i EO og øvrig regelverk.

2.4.1. DELKONKLUSJON – PART 3:

Basert på lovteksten i Part 3, kan det ikke utelukkes at personopplysninger om barn vil bli gjenstand for overvåkning ved bruk av GWE i norske skoler.

3. PRESIDENTIAL POLICY DIRECTIVE 28 (PPD-28)

3.0. BAKGRUNN

PPD-28 ble utstedt i 2014 som et supplerende veiledningsdokument til EO 12333. Hensikten var å modifisere det amerikanske overvåkningsregimet som var autorisert av EO 12333. EO 12333 og PPD-28 skal forstås som veiledningsmateriell for amerikansk overvåkningsvirksomhet på lik linje.

PPD-28 inneholder blant annet prinsipper for informasjonsinnhenting, begrensninger på hvordan bestemte kategorier av kommunikasjon kan brukes, samt restriksjoner på aktørers formidling og tilbakeholding av personopplysninger om «foreigners».[5]

[5] https://www.scribd.com/document/304892216/Overseas-Surveillance-in-an-Interconnected-World#, Brennan Center for Justice, Overseas Surveillance In An Interconnected World, Amos Toh, Faiza Patel, Elizabeth Goitein, Kap. II, bokstav B, s.12

I likhet med EO 12333 (se Part 3), krever PPD-28 at aktører med overvåkningsmyndighet etablerer prosedyrer og rutiner som implementerer prinsippene som følger av gjeldende lovverk (EO 12333 og FISA).[6]

3.1. EGNE PROSEDYRER ("IMPLEMENTING PROCEDURES")

I henhold til PPD-28 Sec. 4, skal aktører med overvåkningsmyndighet etablere egne prosedyrer og rutiner for gjennomføring av overvåkning. Dette åpner for en fullmaktsstruktur som tilsvarer den som knesettes i Part 3 i EO 12333. Prosedyrene skal etableres slik at overvåkningen til enhver tid overholder prinsippene etter EO 12333 og PPD-28, samt øvrige regler, direktiver, proklamasjoner og statutter.[7] Nevnte aktører er også forpliktet til å dokumentere og rapportere at etablerte prosedyrer og rutiner er i overenstemmelse med prinsippene. Rapportering kreves rutinemessig (stort sett årlig).[8]

Under første avsnitt Sec.4 om «Safeguarding Personal Information Collected Through Signals Intelligence», legges det til grunn at ett av hovedhensynene med å etablere prosedyrer er å sikre at «[a]ll persons should be treated with dignity and respect, **regardless of their nationality** or **wherever they might reside**, and **all persons** have legitimate privacy interrests in handling of their personal information.». (mine uthevinger)

Første avsnitt utfylles videre av bokstav (a) til (d). Her beskrives nærmere hvordan prosedyrene skal utformes. Håndteringen av data skal blant annet være i tråd med fire underpunkter, herunder «Minimization(i)», «Data Security and Access (ii)», «Data Quality (iii)», «Oversight (iv)».

3.2. DELKONKLUSJON – PPD-28:

Basert på lovteksten i PPD-28, kan det ikke utelukkes at personopplysninger om barn vil bli gjenstand for overvåkning ved bruk av GWE i norske skoler.

4. EXECUTIVE ORDER 14086 (EO 14086)

4.0. BAKGRUNN

Den Europeiske kommisjonen og amerikanske styresmakter inngikk den 25.mars 2022 en «avtale i prinsippet» om et nytt rammeverk for overføring av personopplysninger mellom EU/EØS og USA.

Som ledd i gjennomføringen av denne avtalen ble USA forpliktet til å etablere nye og utvidede sivile rettigheter opp mot landets etterretnings- og overvåkningsvirksomhet.[9] Executive Order 14086

---

[6] https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities, Sec.4.
[7] EO 14086, Sec. 1 Principles Governing the Collection of Signals Intelligence, bokstav (a) https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities,
[8] EO 14086, Sec. 5 Reports, https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities,
[9] https://www.fieldfisher.com/en/insights/eo-14086-and-the-eu-us-data-privacy-framework

trådte i kraft 7.oktober 2022 og implementerer de nye utvidede rettighetene gjennom rettslige sikkerhetsmekanismer og andre begrensende tiltak. EO 14086 er ment å avløse deler av PPD-28. [10]

4.1. NØDVENDIG OG FORHOLDSMESSIG

I henhold til EO 14086 Sec. 2, nummer (ii), bokstav (A), skal «signals intelligence activities […] be conducted only following a determination, based on a reasonable assessment of all relevant factors, that the activities are **necesarry** to advance a validated intelligence priority.». [11]

Videre følger det av bokstav (B) at «signals intelligence activities shall be conducted only to the extent and in a manner that is **proportionate** to the validated intelligence priority for which they have been authorized.». [12]

Ordlyden i EO 14086 legger opp til samme vurderingstema som ellers er kjent i EU-retten; alle inngrep skal være nødvendig og forholdsmessig i et demokratisk samfunn. Slik sett kan det argumenteres for at de nyetablerte prinsippene legger til rette for generell styrking av vernet av data og personopplysninger i USA.

Hvorvidt dette har reell innvirkning på risikoen forbundet med norske skolers bruk av GWE, er imidlertid vanskelig å svare ut. Graden av innvirkning dikteres av følgende forhold: 1) at beskyttelsen som disse prinsippene medbringer, også tilkjennes EU-borgere på lik linje med «US persons», og 2) at forpliktelsene følges opp i praksis i henhold kravet om «essentially equivalent» beskyttelsesnivå som i EU jf. Schrems II-dommen.

Når det gjelder punkt 1) må det merkes at EO 14086 inneholder samme formulering som PPD-28 om hvem som nyter vern jf. EO 14086 Sec. 1.[13] Slik sett er det grunn til å vurdere den reelle effekten av formuleringen med en viss skepsis – særlig fordi PPD-28 har virket (i alle fall) siden 2014, og det er få holdepunkter som tilsier at regelverket har virket positivt for EU-borgeres rettigheter siden ikrafttredelse (jf. særlig Schrems II-dommen).

Når det gjelder punkt 2) er det ikke tvilsomt at ordlyden i Sec. 2, i teorien, inviterer til en styrking av det generelle rettighetsvernet for private personer utenfor USA. Om dette vil innebære en reell styrking av personvernet i praksis, er likevel vanskelig å konkludere på. Denne usikkerheten skyldes i hovedsak regelverkets begrensede fartstid (ikraftsatt i oktober 2022). Det Europeiske Personvernrådet (EDPB) har også vært tilbakeholdne i denne sammenheng og understreker i sine uttalelser at organet skal monitorere nærmere den praktiske gjennomføringen av prinsippene.[14]

---

[10] https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en, EU-US Data Privacy Framework, avsnitt (125), s.36

[11] EO 14086, Section 2, (ii), bokstav (A), https://www.govinfo.gov/content/pkg/FR-2022-10-14/pdf/2022-22531.pdf

[12] EO 14086, Section 2, (ii), bokstav (B), https://www.govinfo.gov/content/pkg/FR-2022-10-14/pdf/2022-22531.pdf

[13] PPD-28, https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities, tredje avsnitt, EO 14086 https://www.govinfo.gov/content/pkg/FR-2022-10-14/pdf/2022-22531.pdf, Section 1

[14] https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en,

4.2. LOVLIGE OG ULOVLIGE «OBJECTIVES»

Under Sec. 2, bokstav (b) om «objectives» (formål), følger det av bokstav (i) en opplisting av legitime overvåkningsformål.[15] EO 14086 virker ikke å tilføre nye formål ut over det som allerede er etablert i EO 12333. De legitime formålene inkluderer bl.a. styrking av sikkerhet, antiterror, kontraetterretning, m.m.[16] Ordlyden i Sec. 2, nummer (i) inneholder ingen endring i det rettslige handlingsrommet for å velge ut mål, eller å bestemme overvåkningens rekkevidde.

Begrensninger i målutvelgelse og rekkevidde reguleres i nummer (ii). Til forskjell fra EO 12333, avgrenses legitime formål i EO 14086 negativt.Under bokstav (A) listes opp en rekke «Prohibited objectives» - altså formål man *ikke* kan gjennomføre overvåkning etter.

Etter nummer (ii) bokstav (A) følger det at:

*«Signals intelligence collection activities **shall not** be conducted **for the purpose of**:*

(1) suppressing or burdening criticism, dissent, or the free expression of ideas or political opinions by individuals or the press;

*(2) **suppressing or restricting legitimate privacy interests**;*

(3) suppressing or restricting a right to legal counsel; or

(4) disadvantaging persons based on their ethnicity, race, gender, gender identity, sexual orientation, or religion.»

Et relevant spørsmål er derfor om norske skolers bruk av GWE omfattes av reglene om forbudte formål («prohibited objectives»).

Ordlyden av «for the purpose of», tilsier at forbudsbestemmelsen bare omfatter overvåkning der formålet eksplisitt og uttalt er å undertrykke («*suppress*») eller begrense («*restrict*») hensynene som er listet opp.

Forbudsbestemmelsen fremstår på denne måten som lite praktisk anvendbar. Aktører med overvåkningsmyndighet etter EO 12333 vil neppe definere, og enda mindre være åpne om overvåkning begrunnet i et uttalt ønske om å undertrykke, eller ulovlig begrense noens privatliv.

Ordlyden i bestemmelsen avgrenser dermed mot ulovlig formål som i praksis aldri vil kunngjøres av amerikanske overvåkningsaktører. Et rettighetsvern som betinges av denne type vilkår, blir illusorisk. I den grad overvåkningaktører likevel skulle velge å etablere slike formål, er det ikke usannsynlig at formålene vil unntas offentlighet med henvisning til nasjonal sikkerhet.[17]

På denne bakgrunn foreligger det et vesentlig behov for å avklare rekkevidden og omfanget av forbudsbestemmelsen. Følgende problemstilling kan dermed reises;

Er det holdepunkter for å si at forbudet verner mot overvåkning som indirekte eller på utilsiktet måte fører til at norske skolers data i GWE blir innhentet, selv om overvåkningen opprinnelig er etablert i tråd med legitime overvåkningsformål jf. nummer (i), bokstav (A)?

---

[15] Se note 9, Section 2, (a), (i)
[16] EO 12333, bokstav (d) punkt 1-3, s.693, https://www.dni.gov/files/documents/OGC/IC%20Legal%20Reference%20Book%202020.pdf
[17] Se note 2, punkt (1) om «General Principles on Gathering information», s.19

Som nevnt over, gir ordlyden i nummer (ii) bokstav (A) ingen retningslinjer på denne problemstillingen. Noe veiledning kan imidlertid finnes i nummer (iii) bokstav (A) om «Validation of signals intelligence collection priorities».

Under henvisning til Sec. 102A i «National Security Act», plikter «Director of National Intelligence (Director)» å etablere overordnede «prioritites for the Intelligence Community». Formålet med å etablere prioriteringer er å sikre at innhenting av «signals intelligence» til enhver tid er «timely and effective», samt, og kanskje viktigst; i tråd med krav om «legitimate objectives».

Hvorvidt en bestemt overvåkningsaktivitet er i tråd med «legitimate objectives», beror blant annet på en vurdering av om den bestemte overvåkningsaktiviteten er designet for, eller er forventet å resultere i en overtredelse *(«contravention»)* av de forbudte formålene i (ii).[18]

Dersom en bestemt overvåkningsaktivitet på utilsiktet måte resulterer i overtredelse av de forbudte formålene, leses ordlyden i nr. (2) til at slik overvåkning må forbys. At overvåkningen opprinnelig er etablert i henhold til et lovlig formål, vil her være underordnet. Forbudsbestemmelsen oppstiller et vern som i teorien kan være egnet til å ha reell og positiv virkning for EU-borgeres rettigheter. Dette trekker i retning av at norske skolers bruk av GWE omfattes av reglene om forbudte formål.

I fortsettelsen må det imidlertid merkes at anslaget om teoretisk beskyttelse hviler på to særskilte betingelser:

- Forbudet må håndheves i praksis.
- Forbudene må dekke og verne opplysninger som behandles i GWE.

Siden EO 14086 er et nytt regelverk, er det ikke uten videre enkelt å vurdere om, eller i hvilken grad forbudet faktisk vil bli håndhevet.

Når det gjelder forbudets rekkevidde og omfang, er det også en utfordring at vurderingstemaene tilknyttet hvert av forbudene, ikke er kjent. Dette vanskeliggjør øvelsen med å identifisere hvilket ulovlige formål som kan vurderes.

Blant forbudene i bokstav (A), fremstår nr.(2) om «legitimate privacy interest» å være mest aktuelt å vurdere i konteksten av norske skolers data.

Ordlyden av «legitimate privacy interests» virker å dekke mer generelle og uspesifiserte personverninteresser. Hvilke personverninteresser som her omfattes, er derfor uklart. Den samme uklarheten hefter også med begrepet «legitimate». Ordlyden gir ingen veiledning her.

Kombineres manglende veiledning med fullmaktstrukturen som ellers er utbredt i denne type regelverk, er det en rimelig antakelse at innholdet i «legitimate privacy interests» overlates til den enkelte overvåkningsaktør å definere selv, jf. reglene om «implementing procedures» etter EO 12333 og PPD-28.[19]

Skulle denne antakelsen stemme, løper det en betydelig risiko for at forbudene vil håndheves ulikt på tvers av overvåkningsaktørenes virkeområder. Slik sett er det vanskelig å konkludere på spørsmålet om forbudene dekker og verner opplysninger som behandles i GWE. Dette er en usikkerhet som utgjør en betydelig risiko for prosjektet.

---

[18] EO 14086, nr. (iii), bokstav (A), nr. (2), https://www.govinfo.gov/content/pkg/FR-2022-10-14/pdf/2022-22531.pdf

[19] Se note 2, punkt (II), bokstav A og B, «EO 12333 and Implementing Procedures», «PPD-28 and Implementing Procedures».

Det sentrale for prosjektet er ikke å kartlegge hele EO 14086. Det sentrale er å få en bedre forståelse av sannsynligheten for at norske skolers data i GWE blir gjenstand for overvåkning. Konklusjonen vil i hovedsak dikteres av reglene som gjelder for identifisering av mål, hvilke data som er av interesse, og eventuelt hvilke begrensninger overvåkningsaktørene er underlagt.

4.3. TILPASSET OVERVÅKNING

Under Sec. 2, bokstav (c), nummer (i) om «Collection of signals intelligence», følger det av bokstav (B) at:
*«[…]Signals intelligence collection activities shall be as tailored as feasible to advance a validated intelligence priority and, taking due account of relevant factors, not disproportionately impact privacy and civil liberties. Such factors may include, depending on the circumstances, the nature of the pursued objective; the feasible steps taken to limit the scope of the collection to the authorized purpose**; (1)the intrusiveness of the collection activity**, including its duration; the probable contribution of the collection to the objective pursued; **(2)the reasonably foreseeable consequences to individuals**, including unintended third parties; **(3)the nature and sensitivity of the data to be collected**; and the safeguards afforded to the information collected.».*

Bokstav (B) må leses i sammenheng med prinsippene om forholdsmessighet og nødvendighet jf. Bokstav (A) (se punkt 4.2 over).

Bokstav (B) gir veiledning om hvilke momenter som skal vektlegges i vurderingen av om prinsippene blir overholdt. Etter ordlyden i bokstav (B) er det fortrinnsvis tre momenter(uthevet) som etter vår vurdering er egnet til å fange opp de særlige omstendigheter/sensitive karakteren ved norske skolers bruk av GWE.

I den grad disse momentene vektlegges i praksis, er det etter ordlyden i nr.(1),(2) og (3) grunn til å tro at opplysninger om barn vil nyte et forsterket vern.

EO 14086 gir i teorien anvisning på et forsterket beskyttelsesnivå sammenlignet med EO 12333. Det er imidlertid vanskelig å vurdere hvorvidt den teoretiske beskyttelsen kan, og vil, omsettes i den praktiske håndhevingen av lovverket.

4.4. DELKONKLUSJON – EO 14086

Basert på lovteksten i EO 14086, kan det ikke utelukkes at personopplysninger om barn vil bli gjenstand for overvåkning ved bruk av GWE i norske skoler.

5. KONKLUSJON - TEORI

Basert på gjennomgangen av lovteksten i EO 12333, PPD-28 og EO 14086, kan det ikke utelukkes at opplysninger om barn i norske skoler blir gjenstand for overvåkning gjennom bruk av Google Workspace for Education.

6. GJENNOMGANG AV PRAKSIS

6.0. EXECUTIVE ORDER 12333, PPD-28 OG EXECUTIVE ORDER 14086

EO 14086 og adekvansbeslutning for USA ble etablert med en hensikt om å bl.a. begrense omfanget og rekkevidden av overvåkning etter EO 12333. Den overordnede ambisjonen var å harmonere rettstilstanden i EU med rettstilstanden i USA. Av særlig betydning i denne sammenheng er etableringen av prinsippene om forholdsmessighet og nødvendighet. Potensielt innebærer dette et grunnleggende skifte i amerikansk overvåkningsvirksomhet. Tidligere praksis etter EO 12333 vil dermed ha svært begrenset vekt og relevans i denne rapporten. Prosjektet anser det derfor å være en unødvendig øvelse å vurdere dette nærmere.

7. KONKLUSJON – PRAKSIS

På nåværende tidspunkt er det ikke kjent hvordan EO 14086 vil virke sammen med EO 12333 og PPD-28. Slik sett er det verken grunnlag for å avskrive, eller omfavne etableringen av nytt regelverk.

Dette vanskeliggjør muligheten til å konkludere på spørsmålet om det på bakgrunn av praksis på området, er grunn til å tro at norske skolers bruk av GWE blir gjenstand for overvåkning. Men selv om konklusjonen uteblir må det likevel understrekes at fravær av konklusjon på dette spørsmålet, i seg selv, utgjør en usikkerhet og dermed også en risiko for prosjektet.