L218: Matematiske, juridiske og etiske realiteter bag PET's AI-planer

Af praktiserende læge Thomas Birk Kristiansen

Opsummering

- L218 giver PET adgang til at indhente og analysere "større sammenhængende datasæt" fra andre myndigheder uden konkret mistanke mod de omfattede personer. Dette muliggør algoritmisk screening - søgning efter mønstre for at identificere potentielle terrorister, spioner og sabotører.

- L218 angiver ikke størrelsen på de datasæt, PET skal have adgang til, men formuleringen *"som helhed må antages at have betydning"* åbner reelt for datasæt, der kan omfatte hele befolkningen. Selv hvis PET i praksis kun analyserede afgrænsede populationer – f.eks. 1 mio. personer – forbliver et grundlæggende problem: Screening for ekstremt sjældne fænomener vil uundgåeligt generere enorme mængder falske positiver. Det kaldes for base-rate-problemet.

- Ved en AI-specificitet på 95 % vil screening af 1 mio. personer give ca. 50.000 falske alarmer. Udvides det til hele befolkningen på 6 mio., stiger antallet til ca. 300.000. Samtidig vil de reelle tilfælde – f.eks. 6 terrorister – drukne i støjen. Dette base-rate-problem er matematisk uafvendeligt og selv med en hypotetisk AI-nøjagtighed langt over det realistiske vil problemet bestå.

- L218 åbner for, at også sundhedsdata og genetiske oplysninger kan indhentes af PET uden konkret mistanke, uden dommerkendelse og uden danskernes viden. Dermed undergraves både lægers tavshedspligt og den tillid, som sundhedsvæsenet og sundhedsforskningen hviler på.

- Psykiatriske data er uegnede til at forudsige terroradfærd. At give PET adgang vil derfor ikke øge sikkerheden, men derimod stigmatisere og marginalisere mennesker med psykisk sygdom – hvilket i sig selv udgør en sikkerhedsrisiko. Problemet med farlige psykiatriske patienter løses ikke af PET.

- Hvis Folketinget vedtager L218 uændret, risikerer vi at stå med et AI-system, der hverken er egnet, nødvendigt eller proportionalt.

Anbefalinger

- **Indhent dokumentation:** Kræv oversigter over brud på §114–114j (terror-paragrafferne) samt for spionage, sabotage og udenlandske aktører de seneste 25 år – som grundlag for at vurdere base-rate-problemet og derved evt. mangel på AI-træningsdata.

- **Gennemfør AI-teknisk vurdering:** Kræv en uafhængig vurdering af PET's planlagte AI-system og dokumentation for systemets faktiske egnethed, før L218 kan behandles videre.

- **Ved uegnethed:** Indfør målrettede alternativer baseret på konkret mistanke og dommerkendelse**.**

- **Ved egnethed og proportionalitet:** Fastlæg i L218, hvilke datakategorier PET kan indhente, og undtag sundhedsoplysninger, herunder genetiske og psykiatriske oplysninger.

København 30. september 2025.

Kære medlemmer af Folketingets Retsudvalg

Jeg vil gerne takke udvalgets medlemmer for venlig deltagelse, spørgsmål og engagement i forbindelse med mit oplæg ved den åbne høring om en kommende PET-lov den 28. august 2025. Med blot 15 minutter til rådighed var mit oplæg nødvendigvis kortfattet og fokuseret på sundhedsdata. Der er dog bredere og helt fundamentale problemer ved lovforslaget, som jeg vil uddybe her. Brevet er skrevet som privatperson og ikke på vegne af nogen institution, og bør ikke læses som et angreb på hverken Justitsministeriets eller PET's intentioner. Ligeledes skal det ikke læses som teknologifjendtligt eller en generel afvisning af AI i efterretningsarbejde eller andre steder.

Baggrund

Med L218 [1] får PET adgang til at indsamle og analysere større sammenhængende datasæt fra andre myndigheder med henblik på algoritmisk målopdagelse. Data kan opbevares i op til 20 år, og hverken GDPR eller den danske databeskyttelseslov gælder for denne behandling [2,3]. Loven vedrører ikke beslutningsstøtte i konkrete efterforskninger eller ved analyse af allerede mistænkelige netværk, men om bred algoritmisk analyse – altså ved brug af kunstig intelligens (AI) - uden forudgående mistanke.

På høringen i Folketingets Retsudvalg den 28. august 2025 blev det fremført, at dette er nødvendigt for bedre at kunne opspore terrorister, spioner og sabotører samt forebyggede deres eventuelle aktioner – hensyn, der er legitime når det sker for at sikre rigets sikkerhed.

En proportionalitetsvurdering af et indgreb hviler på tre ben, hvor kravet er at et indgreb både skal være:

1) **Egnet**
2) **Nødvendigt**
3) **Proportionalt**

I en sådan vurdering af L218 er problemet, som også blev påpeget ved høringen af Adam Diderichsen fra Forsvarsakademiet, at PET's ønskede AI-system af matematiske grunde har begrænset egnethed. Den matematiske dokumentation indikerer, at det beskrevne set-up derfor ikke kan opfylde egnethedskriteriet. I dette er tilfældet, er der ikke grundlag for at fortsætte proportionalitetsanalysen.

EU-Domstolen har i sager om teledata [4,5] understreget, at selv hensynet til national sikkerhed skal afvejes mod borgernes grundlæggende rettigheder. Selvom L218 ikke falder under EU-domstolens afgørelser om teledata, rejser lovforslagets konstruktion med bred adgang til datasæt lignende principielle spørgsmål om proportionalitet og kontrol. Henvisningen er ikke en påstand om direkte retsanvendelse, men til at principper for proportionalitet og kontrol også gælder ved national sikkerhed.

Endelig har Justitsministeren bekræftet, at sundhedsoplysninger kan indhentes som en del af større datasæt, hvis der foreligger "særligt vægtige hensyn" til PET's opgavevaretagelse, og anerkendt at genetiske oplysninger i den forbindelse rejser særlige spørgsmål [6].

I de følgende afsnit uddybes følgende emner:

1. **Den matematiske realitet: AI-målopdagelse vil uundgåeligt drukne i falske positiver.**
2. **Danske og internationale kilder underbygger, at AI-målopdagelse er uegnet til at fange terrorister.**
3. **Sundhedsdata: Tavshedspligt, psykiatriske og genetiske oplysninger samt forskning.**
4. **Transparensparadokset.**
5. **Indvendinger og diskussion.**
6. **Konklusion.**

Bilag A: Indeholder aktindsigt, der dokumenterer, at overvejelser om genetiske oplysninger og DNA indgik i Justitsministeriets forberedelse af L 218 i otte sager i perioden 2022–2025.

Bilag B: Præsenterer privacy-bevarende teknologier som et konkret alternativ til L218's masseovervågning, hvor sikkerhedsbehov kan imødekommes gennem anonymiseret dataanalyse kombineret med domstolskontrol – en model der respekterer både sikkerhed og borgernes grundlæggende rettigheder.

Bilag C: Belyser tekniske spørgsmål om datasikkerhed og valg af HPC-infrastruktur, som implementeringen af L 218 rejser.

1. Den matematiske realitet: AI-målopdagelse vil drukne i falske positiver

1.1 Målgruppe for L218.

Ifølge lovforslagets bemærkninger er formålet at styrke PET's muligheder for at identificere personer og netværk, der kan true rigets sikkerhed, og retter sig specifikt mod følgende trusselsaktører:

- **Terrorister** – personer involveret i terrorisme og andre sikkerhedstruende aktiviteter.
- **Spioner** – fremmede staters efterretningstjenester og deres agenter, særligt fra Rusland og Kina, men også fra Iran, Tyrkiet og Saudi-Arabien.
- **Sabotører** – aktører, der kan true kritisk infrastruktur og samfundsvigtige funktioner, bl.a. i lyset af Ruslands krig i Ukraine.
- **Udenlandske aktører** – herunder udenlandske staters forsøg på påvirkning af danske interesser, chikane af dissidenter i Danmark samt ulovlig viden- og teknologiindhentning.

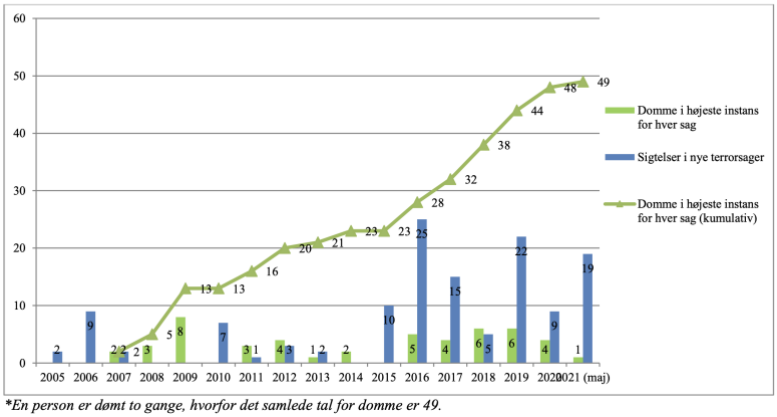
Lovforslaget præciserer, at PET primært håndterer trusler inden for Danmarks grænser, mens ansvaret traditionelt har været delt med Forsvarets Efterretningstjeneste (FE), der fokuserer på trusler udefra.

De aktører, loven retter sig imod, udgør en meget lille del af den danske befolkning. Mange er tilrejsende eller transnationale og vil næppe kunne identificeres effektivt gennem brede analyser af danske befolknings- og registerdata. De følgende matematiske eksempler tager derfor udgangspunkt i terrorister, som er den mest specifikt beskrevne trussel i lovforslaget.

1.2 Domme efter terrorparagraffer i perioden 2001-22:

Terrorsager i Danmark er sjældne. I 2002-2021 blev der afsagt 49 terrordomme (vedrørende 48 personer), og i 2021 sad 39 indsatte med terrorsager i Kriminalforsorgen, se nedenstående figur fra Bjelkegruppens rapport [7]:

BJELKEGRUPPEN UKLASSIFICERET SEPTEMBER 2021



**En person er dømt to gange, hvorfor det samlede tal for domme er 49.*

I 2022 blev yderligere 18 personer dømt efter terrorparagrafferne (§ 114–114 j) – et historisk højt niveau. Hovedparten af disse domme vedrørte dog § 114 j (ulovlig rejse til konfliktzoner) og ikke § 114 om terrorhandlinger. De fleste sager angik fremmedkrigere i Syrien eller støtte til Islamisk Stat [8].

Det er aldrig i Danmark afsagt dom for fuldbyrdet terrorisme efter § 114, stk. 1 [9]. Alle kendte danske terrordomme angår enten forsøg, medvirken til forsøg eller støtte til terrororganisationer. I eksempelvis Krudttønden-sagen (2015) blev gerningsmanden Omar El-Hussein dræbt af politiet og derfor aldrig dømt.

Dog slog Københavns Byret i en dom den 27. september 2016 fast, at Omar El-Husseins handlinger ved Krudttønden og senere ved synagogen var terrorisme, mens fire andre blev frifundet for forsøg på medvirken til terrorhandlinger [10].

I regneeksemplet om terrorister i Danmark nedenfor anvendes et skøn om, at der på et givet tidspunkt findes seks terrorister i Danmark. Det svarer til en forekomst på blot én ud af en million i en befolkning på seks millioner indbyggere.

1.3 Base rate-problemet: PET drukner i falske alarmer

Hvis man vælger at overvåge alle Danmarks seks millioner borgere med AI for at identificere potentielle terrorister, støder man på det såkaldte base-rate-problem. Det samme gælder, selv hvis man begrænser overvågningen til én million. Base-rate-problemet ændrer sig ikke. Samtidig vil en udeladelse af de øvrige fem millioner borgere uundgåeligt betyde, at potentielle terrorister også findes i den udeladte gruppe, fordi ingen filtreringsmetode kan udvælge sikre-ikke-terrorister fejlfrit.

Lad os nu alligevel som eksempel se på AI-overvågning af 6 mio. danskere, hvori der på et givent tidspunkt gemmer sig 6 terrorister. Her løber PET ind i det, der kaldes base-rate-problemet eller *false positive-paradox* [11-13]. Det betyder, at hvis man leder efter noget, som er ekstremt sjældent, vil selv en meget nøjagtig procedure føre til overvældende mange falske alarmer.

Lad os for at forstå problemet se nærmere på sundhedsvæsenet hvor kunstig intelligens har særligt gunstige arbejdsbetingelser: store datamængder, digitaliserede billeddata og veldefinerede diagnoser, som kan verificeres med vævsprøver. Alt sammen forudsætninger, som ikke gør sig gældende når man forsøger at fange terrorister.

Mammografiscreening er inden for sundhed et af de mest modne anvendelsesområder. Men selv AI-mammografiscreening er langt fra at være nøjagtig. Nøjagtigheden måles på de parametre, man kalder for sensitivitet og specificitet. En metaanalyse fra 2023 har rapporteret om en sensitivitet på 80% og en specificitet på 86% for AI-mammografi [14]. Studiet konkluderer, at AI præsterer lige så godt som eller bedre end radiologer i screening for brystkræft med digital mammografi.

Et nypubliceret svenske lodtrækningsforsøg fra 2025 - det såkaldte MASAI-studie [15] – viser performance på niveau med metaanalysen fra 2023 [14]. Studiet inkluderer 105.915 kvinder og peger på øget kræftdetektion, men måske på bekostning af en mindre (ikke signifikant) falsk-positiv rate. Studiet angiver hverken sensitivitet eller specificitet.

Danish Comprehensive Cancer Center (DCCC) påpegede i deres rapport fra 2024 [16], at selv ved mammografiscreening – et af de mest modne AI-anvendelsesområder med standardiserede data og veldefinerede mål – er der betydelige udfordringer og rapporten understreger behovet for løbende kvalitetssikring og ekstern validering.

Selv under næsten ideelle medicinske betingelser formår AI altså ikke at overstige 80-86% på begge parametre samtidigt. Det gør det urealistisk at forvente, at AI kan identificere potentielle terrorister med større nøjagtighed i komplekse sociale sammenhænge, hvor base-raten ligger i størrelsesordenen 1 ud af 1 million. Alligevel sætter vi PETs tænkte AI-system til en nøjagtighed på 95% på begge parametre.

Tænkt scenarie for AI-målopdagelse af terrorister

- **Population:** 6.000.000 danskere
- **Reelle terrorister:** 6 personer
- **Modelpræcision:** 95 % sensitivitet, 95 % specificitet (urealistisk højt estimat)

Resultat (forventede værdier):

- **Sande positive (TP):** $6 \times 0{,}95 = 5{,}7 \approx 6$
- **Falske negative (FN):** $6 \times 0{,}05 = 0{,}3$ (≈ 0–1)
- **Sande negative (TN):** $(6.000.000 - 6) \times 0{,}95 \approx 5.699.994$
- **Falske positive (FP):** $(6.000.000 - 6) \times 0{,}05 = 299.999{,}7 \approx 300.000$

Positiv prædiktiv værdi (PPV): $PPV = 5{,}7 / (5{,}7 + 300.000) \approx 0{,}002\ \%$

Med andre ord: For hver én reel terrorist, som AI-systemet identificerer korrekt, vil omkring 50.000 uskyldige borgere fejlagtigt blive mistænkeliggjort. Det illustrerer base-rate-problemet og understreger PET's planlagte AI-systems praktiske uanvendelighed.

Selv ikke en uhørt høj sensitivitet og specificitet på 99% ville fjerne base-rate-problemet, fordi det for hver én reel terrorist ville udpege 10.000 uskyldige borgere**.** Og selv et fiktivt AI-system med uhørt nøjagtighed vil derfor være uanvendeligt. Og så skal vi endda huske at også en nøjagtighed på 95% er et uhørt optimistisk estimat for et så komplekst og ubalanceret problem.

Base-rate-problemet er matematisk uomgængeligt. I praksis betyder det, at tusindvis af uskyldige borgere vil blive gjort til genstand for efterforskning. Det undergraver både retssikkerheden og borgernes tillid til myndighederne

1.4 Når flere data gør problemet værre

Nogle vil hævde, at flere data og mere computerkraft kan løse base-rate-problemet. Men fundamentale matematiske begrænsninger gør, at problemet består, så længe den underliggende forekomst af hændelsen (f.eks. terrorisme) er ekstremt lav.

Når målet er at udpege en bestemt risikoprofil eller et tilhørsforhold ved hjælp af store sammenhængende datasæt, benyttes typisk AI-metoder baseret på højdimensionel statistik [17-19]. Her gælder særlige lovmæssigheder, blandt andet at beregningskompleksiteten i højdimensionale rum vokser eksponentielt med antallet af variable. Dette skyldes den såkaldte dimensionalitetsforbandelse ("curse of dimensionality"), som Bellman beskrev allerede i 1957 [20]. Den beskriver, at data "fortyndes" i højdimensionale rum. Jo flere variable der inddrages, desto mere spredes datapunkterne, og desto sværere bliver det at identificere meningsfulde mønstre.

Hughes dokumenterede i 1968, at den såkaldte klassifikationspræcision i begyndelsen stiger med flere variable, men efter et optimalt punkt falder den hurtigt igen [21]. Dette gælder ikke kun for klassifikation, men også for regression og clusteranalyse. Med andre ord, der kræves eksponentielt flere træningseksempler, når antallet af variable i en model øges.

I en terrorbekæmpelseskontekst bliver dette katastrofalt. Danmark har meget få kendte terrorsager, men potentielt tusindvis af variable i sammenkoblede registre – sociale medier, teledata, sundhedsdata, skatteoplysninger osv. Kombinationen af meget høj dimensionalitet og meget få træningseksempler fører til overfitting og lav generaliserbarhed [17-19]. Dermed kan mere data og større regnekraft ikke afhjælpe base-rate-problemet – men derimod forværre dets konsekvenser.

I højdimensionelle rum opstår uundgåeligt tilfældige og spuriøse mønstre. En forretningsrejsende markeres for hyppige mellemlandinger i Istanbul. En landmand vækker mistanke ved sæsonvise gødningskøb. Tilfældige sammenfald om handelsvaner eller brug af offentlig transport kan blive fejlagtigt tolket som meningsfulde signaler. Med tusindvis af variable stiger risikoen for falske koblinger eksponentielt, og modellerne begynder at "se mønstre", der reelt er støj [20,21].

Selv moderne AI-modeller rammes desuden af underspecificering: To modeller kan præstere næsten identisk på testdata, men opføre sig radikalt forskelligt i praksis, fordi de har lært forskellige – ofte irrelevante eller diskriminerende – mønstre fra træningsdata. Resultatet er systemer, der ser robuste ud under kontrollerede forhold, men fejler i virkelige applikationer — og i værste fald udpeger vilkårlige grupper som "mistænkelige", hvor langt de fleste er uskyldige [22]. Problemet forværres yderligere, når træningsdata er sjældne eller ubalancerede, fordi modellerne mangler tilstrækkelige eksempler til at skelne reelle signaler fra støj.

1.5 Fejl i data

Det er ikke kun de statistiske begrænsninger, der underminerer PET's AI-planer. En anden afgørende svaghed er datakvaliteten. Selv når data er tekniske og tilsyneladende neutrale, rummer de ofte alvorlige fejl. Kvaliteten af data er bredt anerkendt som en akilleshæl for kunstig intelligens, og problemet bliver ofte større, når data genanvendes til andre formål end det formål data oprindeligt blev indsamlet til [23,24].

National Institute of Standards and Technology (NIST) har understreget dette: resultater, der ser lovende ud i kontrollerede forsøg, kan afvige, når systemerne anvendes i den virkelige verden [23].

Fænomenet *data cascades* er særligt bekymrende. Her betyder små fejl i indsamling, registrering eller samkøring af data, at fejl og bias akkumuleres og forstærkes gennem systemet — f.eks. når en algoritme trænes på data, der allerede indeholder fejl, og derefter reproducerer og forstærker disse fejl i sine forudsigelser. I en international undersøgelse af højrisiko-AI rapporterede 92 % af erfarne AI-praktikere, at de havde oplevet mindst én sådan kaskade, og næsten halvdelen havde oplevet to eller flere [25]. Allerede i 1990'erne påviste forskere, hvordan datakvalitetsproblemer kan propagere og skabe systematiske fejl [26]. Når problemet kan dokumenteres på tværs af højrisikodomæner som sundhed og sikkerhed og har været beskrevet siden 90erne, er det forventeligt at PET – med begrænset eksterne kontrol og begrænsede ressourcer til at kuratere data – vil stå over for betydelige udfordringer.

Danske erfaringer dokumenterer også, at selv nogle af de mest centrale registre langt fra er fejlfrie:

- **Lokationsdata**: I 2019 blev hundredvis af sager droppet eller genoptaget, fordi mobiloplysninger ofte viste sig at være fejlfyldte [27,28]. Politiken kunne samme år påvise fejl på helt op til 100 kilometer, hvor telefoner tilsyneladende "sprang" fra ét sted i landet til et andet på sekunder [29].

- **Sundhedsregistre**: En analyse fra almen praksis viste, at omkring 14 % af patienterne var fejlagtigt kodet som type 2-diabetikere [30]. Et andet studie fandt tilsvarende unøjagtigheder i det nationale diabetesregister [31]. For medfødte hjertesygdomme viste en validering, at mere end en tredjedel af registreringerne var forkerte [32].

- **Ejendomsvurderinger**: I 2024 udtalte Ombudsmanden skarp kritik af foreløbige vurderinger, der var så skæve, at de undergravede borgernes tillid [33]. DR dokumenterede i samme periode, at Bygnings- og Boligregistret (BBR) indeholdt massive fejl baseret på 190.000 tilstandsrapporter [34]. Skatteministeriet har desuden oplyst, at ejendomsvurderings-systemet samlet set har kostet omkring 4,5 mia. kr. [35].

Hvis selv et simpelt system til ejendomsvurdering ikke kan levere præcise og pålidelige resultater, hvorfor skulle et langt mere komplekst AI-setup hos PET kunne gøre det bedre? Dårlige data underminerer ikke bare kvaliteten; de svækker projektets anvendelighed. Ingen AI-algoritme eller supercomputer kan ophæve de svagheder, der følger af fejlbehæftede data. AI er ikke magi.

1.6 Problemet med at definere "terrorister"

Selv hvis vi ser bort fra de matematiske og tekniske begrænsninger ved sjældne begivenheder og fejlbehæftede data, står PET's planlagte AI-system over for en grundlæggende udfordring: Hvad er en "terrorist"?

Der findes ikke én entydig profil. En enlig radikaliseret person, der planlægger et angreb fra sit køkken, har intet til fælles med en trænet terrorist med forbindelser til internationale organisationer. En separatist, der kæmper for regionalt selvstyre, opererer på helt andre måder end en cyberkriminel. Nogle drives af religiøse overbevisninger, andre af politisk ideologi, personlige problemer, desperation eller pludselige indskydelser.

Hver type kræver sine egne data, sine egne analysemetoder og en specifik kontekst for overhovedet at kunne genkendes. AI-systemer forudsætter relativt homogene klasser for at kunne lære effektivt. Når

målet derimod er så vagt og heterogent defineret, bliver det umuligt at validere, om systemet faktisk finder det rigtige – eller blot forstærker tilfældige mønstre i støjende data.

1.7 Hvorfor 95 % nøjagtighed er urealistisk: Bayes-optimal classifier og erfaringer fra predictive policing

Selv hvis vi ser bort fra alle praktiske udfordringer og forestiller os perfekte data og ubegrænset regnekraft, vil algoritmisk terroridentifikation stadig støde på en teoretisk mur. *Bayes optimal classifier* er den bedst mulige prædiktive model, givet de tilgængelige data. Den definerer samtidig en ufravigelig nedre grænse for fejl – kaldet *Bayes error rate* – som ingen algoritme, uanset kompleksitet eller datamængde, kan overskride, givet den iboende usikkerhed i data [18,19]. Med andre ord: selv under ideelle betingelser vil enhver metode til prædiktion have en grænse for nøjagtighed, som ikke kan krydses.

I domæner præget af stor heterogenitet – som terrorbekæmpelse – ligger den nedre grænse for fejl højt. Terrorister udgør ikke en homogen gruppe, og denne variation betyder, at selv den teoretisk bedst mulige AI-model i dette domæne vil have markant lavere nøjagtighed end AI-modeller i domæner med klare og veldefinerede klasser.

Erfaringerne fra *predictive policing* – det man også kan kalde for individbaserede risikomodeller i strafferetten – understreger pointen. Her arbejder man med tusindvis af årlige hændelser, omfattende historiske data og langt mere veldefinerede kriminalitetskategorier end ved terror. På trods af store datasæt og relativt veldefinerede udfald ligger performance ofte kun på AUC ≈ 0,6–0,75 i uafhængige studier [36]; udbredte værktøjer som COMPAS ligger typisk omkring ~0,70 [37]. Disse niveauer betyder, at modellerne kun er moderat bedre end tilfældighed til at rangordne højrisiko-individer [38]. En AUC på 0,7 betyder at modellen kun korrekt rangerer en højrisiko-person over en lavrisiko-person i 70% af tilfældene.

Den reelle nøjagtighed for et PET AI-system vil derfor ligge langt under de 95 % i sensitivitet og specificitet, som optimistisk blev anvendt i regneeksemplerne, og formodentlig ikke bedre end ved predictive policing.

Selv hvis man antager 70–80 % specificitet (og sensitivitet) – stadig urealistisk højt givet domænets kompleksitet – bliver konsekvenserne katastrofale. Ved 70 % specificitet ville systemet generere omkring 1,8 millioner falske positive, ved 80 % specificitet omkring 1,2 millioner, hvis det appliceres på 6 millioner borgere. Systemet ville altså fejlagtigt udpege mellem en femtedel og en tredjedel af den danske befolkning som potentielle terrorister.

Dette er ikke blot et spørgsmål om ressourcespild – det er en fundamental undergravning af retssikkerheden. Som Forbes Technology Council konkluderede i oktober 2024, forbliver prædiktion af individuel kriminel adfærd "*beyond the capabilities of AI*" [39].

2. Danske og internationale kilder underbygger, at AI-målopdagelse er uegnet til at fange terrorister

2.1 Politiforsker ved forsvarsakademiet Adam Diderichsen

Adam Diderichsen, lektor i efterretning ved Forsvarsakademiet og også deltog i høringen i retsudvalget, skriver i en kronik i Politiken i april 2025 [40] at der ikke findes eksempler på, at efterretningstjenester eller politikorps har haft succes med at bruge dataanalyse af store datasæt til at identificere terrorister. Problemet er matematisk: selv med optimistiske antagelser om høj præcision vil der altid være så få terrorister i en befolkning, at systemerne drukner i falske positive. Det betyder, at titusinder af uskyldige borgere identificeres fejlagtigt for hver reel mistænkt, hvilket fører til enormt ressourcespild og potentielt

undergraver kampen mod terror. Diderichsen fremhæver også, at de fleste af dem systemet ville udpege korrekt, allerede er kendt af myndighederne, og at gevinsten derfor er minimal. Resultatet bliver et ineffektivt system, hvor efterforskere spilder tiden på at afklare fejlagtige spor frem for at styrke de metoder, der faktisk virker.

2.2 AI-forsker ved Rockwool Fonden Daniel Juhász Vigild

Daniel Juhász Vigild, som er ph.d.-studerende og forsker i AI ved Rockwool-fonden, peger i et debatindlæg i aug. 2025 [41] på en anden grundlæggende svaghed: mangel på data. Kunstig intelligens kræver enorme mængder af træningsdata, og de succesfulde gennembrud med AI – fra kræftdiagnostik til spil som skak og GO – har netop været baseret på millioner af eksempler på det, systemerne skulle lære at forudsige. PET har derimod kun ganske få eksempler på terror, sabotage eller spionage i Danmark, men millioner af eksempler på borgere, der ikke udgør en trussel. Det giver en massiv klasse-ubalance, som gør det umuligt at træne pålidelige modeller. Erfaringer fra udlandet med såkaldt *predictive policing* viser tilsvarende, at teknologien ikke reducerer kriminalitet, men ofte forstærker diskrimination og retssikkerhedsproblemer**.**

2.3 International forskning: Udfordringer ved maskinlæring til terrorbekæmpelse

Verhelst et al. (2020) [42] analyserer, hvorfor maskinlæring har fundamentale begrænsninger, når det anvendes til at identificere terrorister gennem masseovervågning. De peger på tre centrale problemområder:

1. **Ekstrem dataubalance**: Terrorangreb er yderst sjældne begivenheder. Blandt millioner af borgere findes kun ganske få potentielle terrorister. Maskinlæring fungerer bedst, når der er en vis balance mellem de grupper, der skal skelnes imellem, men her er forholdet så skævt, at selv en algoritme med 99,9 % nøjagtighed vil producere tusindvis af falske positiver. Resultatet er, at et stort antal uskyldige personer vil blive udpeget som potentielle trusler, mens den reelle evne til at finde de få farlige individer forbliver yderst begrænset.

2. **For mange variable at analysere**: Terrorangreb varierer enormt – fra enlige ulve til organiserede netværk, fra religiøse til politiske motiver, fra onlineplanlægning med krypterede beskeder til offline aktiviteter i det skjulte. Hver variant kræver analyse af forskellige typer data og nye variable. Jo flere variable algoritmen skal håndtere, desto sværere bliver det at opretholde præcision, især når antallet af reelle eksempler er ekstremt lavt. Kombinationen af høj kompleksitet og få positive eksempler gør det statistisk umuligt at skabe robuste modeller.

3. **Spuriøse mønstre**: Når algoritmer analyserer tusindvis af variable på baggrund af meget få eksempler, finder de uundgåeligt tilfældige sammenhænge, som i virkeligheden er meningsløse – f.eks. at en bestemt skostørrelse eller en bestemt buslinje korrelerer med terrortrusler. Sådanne falske mønstre kan få modellen til at præstere godt på testdata, men vil bryde sammen i virkelige anvendelser. Det giver en farlig illusion af præcision, mens uskyldige borgere risikerer at blive fejlagtigt stemplet som mistænkelige.

Den overordnede konklusion hos Verhelst et al. er, at disse problemer ikke kan løses med flere data eller mere avancerede algoritmer. Tværtimod understreger Verhelst, at vi ikke engang kan forudsige, hvor godt maskinlæringssystemer (ML) vil performe i en befolkning – kun hvor godt de performer på et testdatasæt.

3. Sundhedsdata: Tavshedspligt, psykiatriske data, genetiske data og forskning.

3.1. Tavshedspligt og tillid: Fundamentet for et velfungerende sundhedsvæsen

Læge-patient-forholdet bygger på et løfte om fortrolighed, som gennem generationer har været ukrænkeligt. Hvis PET får adgang til genetiske data, psykiatriske diagnoser og andre sundhedsdata, risikerer vi at underminere selve fundamentet for patienters tillid til sundhedsvæsenet.

Forskning viser, at bekymring om sikkerhed og privatliv får patienter til at tilbageholde sundhedsoplysninger fra behandlere [43]. Selvom befolkningen generelt støtter deling af sundhedsdata til forskning, falder opbakningen markant ved kommercielle eller blandede formål [44]. Tilliden hviler på forventningen om, at data bruges til sundhedsformål [45,46].

Konsekvenserne kan blive alvorlige: patienter, der holder tilbage med vigtige oplysninger, borgere, der undlader at søge nødvendig lægehjælp, og sårbare grupper, der forsvinder fra sundhedsvæsenets radar.

Særligt udsatte borgere rammes hårdt. Personer med psykiske lidelser, misbrugsproblemer eller hvis det generelt lever, på kanten af samfundet kan undlade at søge behandling, hvis de frygter, at deres oplysninger kan ende i efterretningstjenestens databaser. Netop disse er blandt dem, der har mest brug for sundhedsvæsenets hjælp.

PET-loven repræsenterer derfor ikke blot en justering, men et fundamentalt brud med hidtidig praksis. Hvor tavshedspligten i dag kun kan brydes under helt særlige omstændigheder og med streng kontrol, åbner L218 for PET's adgang til sundhedsdata uden patientens samtykke eller viden, uden konkret mistanke om lovovertrædelse, uden uafhængig domstolskontrol og uden efterfølgende underretning.

Hvis tilliden svigter, vakler hele sundhedssystemet. Spørgsmålet er derfor ikke kun, om vi skal beskytte samfundet mod trusler, men også om vi er villige til at ofre læge-patient-fortroligheden – og dermed fundamentet for et velfungerende sundhedsvæsen.

3.2 Psykiatriske data: Uegnede til at sikre rigets sikkerhed

Under høringen i Folketingets Retsudvalg den 28. august 2025 om L218 pegede både justitsminister Peter Hummelgaard og PET's chefjurist Morten Duus-Larsen på, at psykiatriske data kan hjælpe med at identificere masseskydere eller terrorister.

Forskningen viser det modsatte. En Campbell-metaanalyse fra 2022 – gennemført bl.a. i samarbejde med US Homeland Security baseret på 56 studier, 73 samples og i alt 13.648 personer – finder ingen dokumentation for, at terrorister generelt har højere forekomst af diagnosticerede psykiske lidelser end baggrundsbefolkningen. I flere estimater er forekomsten endda lavere [47].

Kun i en snæver undergruppe – såkaldte *lone-actor-terrorists* – ses en tendens til overrepræsentation af psykiske vanskeligheder som personlighedsforstyrrelser og depressive symptomer. Men datagrundlaget er spinkelt og præget af alvorlige metodiske svagheder. Og selv her kollapser logikken: I Danmark er der højst tale om 0–2 lone-actors årligt, mens omkring 10% af befolkningen lever med psykisk lidelse. At bruge psykiatriske data som screeningsredskab ville derfor generere tusindvis af falske positiver for hver enkelt potentiel trussel. Resultatet ville være metodisk ubrugeligt og retssikkerhedsmæssigt katastrofalt.

Brugen af psykiatriske data vil samtidig stigmatisere en i forvejen udsat gruppe. Mange med psykiske problemer er allerede blandt de mest marginaliserede i Danmark. Ved de alvorlige psykiske lidelser er der endda tale om at mange tvangstilbageholdes, tvangsbehandles og tvangsfiksere. At udlevere journaloplysninger om psykisk sygdom til PET vil ramme dem disproportionalt hårdt og kan stride mod diskriminationsforbuddet i dansk ret, EMRK-artikel 14 [48] samt FN's handicapkonvention [49].

Konsekvenserne er forudsigelige og kan illustreres med tænkte eksempler:

- En ung mand med begyndende paranoia og radikaliseringstanker kunne undlade at søge behandling af frygt for registrering – hans sygdom forværres.

- En kvinde med selvmordstanker og vrangforestillinger kunne holde sig væk fra psykiatrien, fordi hun frygter, at hendes paranoia bekræftes – hun forbliver ubehandlet.

- En tidligere radikaliseret, der ønsker psykologhjælp til at forlade sit miljø, kunne vælge at blive i det, fordi risikoen for PET-registrering føles større end gevinsten.

Ironisk nok risikerer PET's adgang til psykiatriske data derved at skabe den form for ustabilitet og fare, som L218 søger at forebygge. Problemet med farlige psykiatriske patienter løses ikke af PET.

3.3. Genetiske data: Total befolkningsidentifikation uden retssikkerhed

Under gældende ret kræver politiets adgang til genetiske data i Nationalt Genom Center efter Sundhedslovens § 223 b, stk. 2 tre betingelser: 1) konkret mistanke, 2) at der er tale om efterforskning af en overtrædelse af straffelovens § 114 eller § 114 a, og 3) dommerkendelse [48]. Retshåndhævelsesloven § 10 bekræfter den særlige beskyttelse af følsomme personoplysninger herunder genetiske data [51].

L 218 ændrer dette billede markant. Ved at definere genetiske data som del af "større sammenhængende datasæt" kan PET indhente dem efter intern vurdering af "særligt vægtige hensyn" – uden konkret mistanke og uden domstolskontrol. Det bekræftes af ministeriets eget svar på spørgsmål til Retsudvalget [6]. Dog vedkender ministeren, "at behandlingen af genetiske oplysninger rejser nogle helt særlige spørgsmål og overvejelser, og at der som konsekvens heraf kan være behov for særskilt at adressere dette i lovforslaget" [6].

Det reelle omfang af genetiske oplysninger i Danmark er massivt, hvor der rådes over omfattende genetiske ressourcer spredt på mange systemer, herunder:

- **Nationalt Genom Center**: ≈ 40.000 helgenomer [52]

- **Regionale patientjournaler**: store dele af NGCs helgenomdata ligger tilgængeligt i EPJ-systemer eller i tekniske undersystemer under regionalt dataansvar.

- **Computerome:** > 500.000 DNA-chipdata [53]. Dataansvarlig: Diverse forskningsprojektejere, som oftest er Region Hovedstaden.

- **iPSYCH:** ≈ 140.000 hælprøver analyseret med DNA-chip uden informeret samtykke [54,55]. Dataansvarlig: Aarhus Universitet.

- **Andre forskningsdatabaser** herunder genetiske data fra universitetsprojekter.

PET behøver derfor ikke direkte adgang til NGC for at få adgang til helgenomer, fordi de samme genetiske data kan indhentes regionalt som "sammenhængende datasæt" – uden de begrænsninger, som § 223 b, stk. 2 ellers pålægger. Derudover er der alle DNA-chipaflæsningerne.

Med moderne slægtskabsanalyse kan de danske genetiske datasæt i praksis bruges til at identificere næsten hele befolkningen – enten direkte eller indirekte gennem genetiske match. Ved hjælp af imputation, en velafprøvet metode [56], kan manglende genetisk information udledes fra slægtninge, så de "manglende brikker" udfyldes. Dermed kan også borgere, der aldrig har fået foretaget genetisk testning, identificeres gennem genetiske data fra deres slægtninge. Retsgenetisk brug af DNA – herunder slægtskabsbaseret identifikation – er allerede en realitet i dansk politiarbejde.

Justitsministeriet har i forbindelse med aktindsigt bekræftet, at genetiske oplysninger har indgået i forberedelsen af L 218. En søgning i ministeriet på nøgleordene *'genetisk'* og *'genetiske'* har nemlig identificeret dokumenter i otte forskellige sager mellem 2022 og 2025 som alle vedrører L218. Dokumentoversigten er vedlagt som Bilag B.

3.4. Risiko for Danmarks position inden for sundhedsforskning

Danmarks position som en førende nation inden for sundhedsforskning og registerbaseret epidemiologi bygger blandt andet på danskernes og det internationale forskningssamfunds tillid til vores databeskyttelse og forskningsetik. Denne tillid er allerede under pres. *Science*, et af verdens mest prestigefyldte videnskabelige tidsskrifter, bragte i august 2025 en nyhedsartikel i sin redaktionelle sektion: '*Blood taken from Danish babies ended up in huge genetic study—without consent*' [55]. Artiklen beskrev, hvordan 140.000 danske børns genetiske data via hælblodprøver er blev analyseret uden forældrenes viden eller samtykke i iPSYCH-projektet. Derved rejste Science international kritik af dansk forskningsetik.

Hvis PET får bred adgang til forskningsdata og herunder genetiske data, risikerer vi at undergrave fundamentet for dansk sundhedsforskning:

- **Forskningssamarbejder kan blive udfordret**: Internationale forskere og institutioner kan blive tilbageholdende med at dele data eller indgå i projekter, hvis de ikke kan garantere deres deltagere, at data ikke vil blive indhentet af PET.

- **Kliniske forsøg kan blive påvirket**: Farmaceutiske virksomheder skal kunne garantere forsøgsdeltagere fortrolighed. Usikkerhed om PET's dataadgang kan gøre Danmark mindre attraktiv for internationale aktører.

- **Informeret samtykke bliver problematisk**: Hvordan skal forsker informere deltagere om databrug, hvis PET kan få adgang uden deres viden? Dette udfordrer grundlæggende forskningsetiske principper.

- **Etiske komitéers vurderingsgrundlag undergraves**: Videnskabsetiske komitéer kan under visse omstændigheder godkende registerforskning uden eksplicit samtykke, når samfundsnytten er betydelig og risici minimale. Men hvordan kan komitéerne vurdere, om risici er "minimale", hvis de ikke kan garantere, at data ikke kan indhentes af PET? Komitéloven forudsætter en proportionalitetsvurdering baseret på forudsigelig dataanvendelse – en forudsætning der forsvinder, hvis PET kan få adgang uden domstolskontrol og uden oplysningspligt herom.

- **Tilliden til danske registre kan svækkes**: Danmarks unikke registerdata er værdifulde netop fordi borgerne har tillid til systemet. Hvis denne tillid eroderes, kan det påvirke datakvaliteten.

Det paradoksale er, at vi i forsøget på at beskytte rigets sikkerhed risikerer at skade Danmarks position som et troværdigt sted at bedrive sundhedsforskning – en position, der har taget årtier at opbygge, og har betydelig værdi både videnskabeligt og samfundsøkonomisk.

4. Transparensparadokset

L218 åbner for fremadrettet algoritmisk screening uden konkret mistanke. Netop fordi der er tale om generel dataindsamling og ikke igangværende efterforskning, udgør det ingen operationel risiko at præcisere, hvilke datatyper PET får adgang til.

Terrorister må allerede antage, at PET kan indhente data. De planlægger ikke angreb ud fra, hvilke registre der er undtaget. Derimod skaber uklarheden usikkerhed for millioner af borgere, som ikke ved, om deres psykiatriske journaler, genetiske oplysninger eller andre følsomme data kan blive genstand for algoritmisk analyse.

Danmark har en tradition for åben regulering: siden 2006 har reglerne om teledata og lokationsregistrering været offentligt beskrevet, og politiets DNA- og fingeraftryksregistre er ligeledes reguleret i åben lovgivning. Denne transparens har ikke svækket politiets arbejde. På samme måde afslører viden om, at PET kan tilgå sundhedsdata, ikke noget om, hvordan data analyseres – ligesom kendskab til DNA-registret ikke afslører politiets efterforskningsmetoder.

Den reelle sikkerhedsrisiko ligger et andet sted: i mistilliden. Hvis borgere ikke kan stole på sundhedsvæsenets fortrolighed, vil nogle undlade at søge behandling. Hvis forskere ikke kan garantere anonymitet, falder forskningsdeltagelsen. Mistillid svækker samfundet – ikke terroristerne.

Løsningen er enkel: Folketinget bør specificere, hvilke datatyper L218 omfatter – fx genetiske oplysninger, psykiatriske journaler og skatteoplysninger – men holde de operative detaljer fortrolige. Elastiske formuleringer som "særligt vægtige hensyn" bidrager ikke til sikkerheden; de undergraver blot den demokratiske kontrol.

5. Indvendinger og diskussion

En oplagt indvending kunne være, at der er flere end seks terrorister i Danmark, og at regnestykket derfor undervurderer den praktiske nytteværdi af algoritmisk målopdagelse. Men selv hvis antallet af mål tidobles til 60 personer, ændrer billedet sig kun marginalt:

- **Sande positive (TP):** $60 \times 0{,}95 = 57$
- **Falske positive (FP):** $(6.000.000 - 60) \times 0{,}05 = 299.997$
- **Positiv prædiktiv værdi (PPV):** $57 / (57 + 299.997) \approx 0{,}019\ \%$ (≈ 1 ud af 5.300)

Selv hvis PET vil lede efter 600 som måske en dag kan blive til terrorister vil der stadig være:

- **Falske positive (FP)**: $(6.000.000 - 600) \times 0{,}05 = 299.700$

Selv hvis antallet af potentielle terrorister tidobles eller hundreddobles, vil langt størstedelen af de personer, der udpeges som mistænkelige, være uskyldige. Ved meget lav base-rate vil systemet altid

generere hundredtusinder af falske alarmer. Dermed forbliver metoden praktisk talt uanvendelig — også under langt mere gunstige forudsætninger end de realistiske.

Man kan også foreslå at filtrere befolkningen og udelukke lavrisikogrupper (fx børn <12 år og borgere >80 år). Selv hvis screeningspopulationen reduceres fra 6 mio. til 4 mio., giver en specificitet på 95 % stadig omkring 200.000 falske alarmer. Problemet er matematisk og lader sig ikke eliminere gennem simple afgrænsninger.

En tredje indvending er, at AI kan have værdi i snævre, mistankebaserede kontekster – fx analyse af allerede identificerede netværk, verifikation af konkrete trusler eller mønstergenkendelse i særlige datatyper.

- **Hvis formålet eksempelvis er, at PET først identificerer 600 personer, der kan være i risiko for radikalisering, og derefter anvender AI-værktøjer og sammenkoblede datasæt til at kvalificere denne vurdering, skal formålet fremgå af lovteksten.**

En sådan målrettet anvendelse er imidlertid ikke beskrevet i L218. Lovforslaget etablerer i stedet adgang til "større sammenhængende datasæt" til brug for algoritmisk målopdagelse uden forudgående mistanke. Argumenter om AI's nytte i konkrete, mistankebaserede efterforskninger er derfor irrelevante for den brede screening, som L218's nuværende formulering muliggør.

Erfaringen viser desuden, at når data først er indsamlet, udvides anvendelsesformålene næsten uundgåeligt – et fænomen kendt som *function creep* [57,58]. Koops definerer function creep som *"an imperceptibly transformative and therewith contestable change in a data-processing system's proper activity"* [57]. Netop det umærkelige er problemet: udvidelsen sker gradvist gennem administrative beslutninger snarere end eksplicitte demokratiske valg, hvilket gør den vanskelig at opdage – og endnu sværere at standse.

- **L218's konstruktion med elastiske kriterier som "særligt vægtige hensyn" gør loven særligt udsat for glidebaneudvikling. Hvad der indføres som terrorbekæmpelse, kan senere og helt umærkeligt udvides til organiseret kriminalitet, økonomisk kriminalitet eller andre samfundsproblemer uden ny folketingsbehandling. Når først infrastrukturen er etableret, bliver argumentet "vi har allerede systemet" en kraftig driver for videre anvendelse.**

Derfor bør L218 kun implementeres efter en solid proportionalitetsvurdering og med klart afgrænsede anvendelsesrammer og robust demokratisk kontrol – ikke med elastiske formuleringer, der i praksis åbner for administrativ udvidelse uden eksplicit parlamentarisk godkendelse af hver udvidelse.

Uden dokumenteret effektivitet er L218 et eksperiment, hvor de matematiske realiteter taler imod succes. Hvis Folketinget vil give PET nye værktøjer, må de være egnede, nødvendige og proportionale. AI-baseret masseovervågning fejler allerede på det første kriterium.

6. Konklusion

Folketinget bør grundlæggende revurdere PET-loven. Hvis PET via L218 skal have adgang til følsomme persondata i store sammenhængende datasæt uden konkret mistanke, må der først foreligge en fyldestgørende redegørelse anvendeligheden og de matematiske forudsætninger for det påtænkte AI-system.

Justitsministeriets rapport om erfaringerne med PET-loven anføres som faglig begrundelse for L218, men den adresserer ikke de fundamentale matematiske og metodiske begrænsninger ved AI-baseret målopdagelse [59].

Terrorbekæmpelse næsten det værst tænkelige domæne for algoritmisk analyse. Terrorisme er et komplekst socialt fænomen påvirket af utallige variable, hvoraf mange er iboende uforudsigelige.

AI er et kraftfuldt værktøj, men dets anvendelighed afhænger kritisk af konteksten. Mens det er ved at være modent inden for veldefinerede medicinske domæner (f.eks. mammografi), er det fundamentalt uegnet til komplekse, sjældne, og subjektive problemer som terrorbekæmpelse. Matematiske, tekniske og etiske begrænsninger må anerkendes for at undgå skadelige og ineffektive implementeringer.

Hvis Folketinget vedtager L218 uændret, risikerer vi at stå med et AI-system, der hverken er egnet, nødvendigt eller proportionalt. Og hvis PET's påtænkte AI-anvendelse inden for L218's rammer ikke omfatter algoritmisk målopdagelse uden konkret mistanke baseret på store sammenhængende datasæt, må de alternative formål meldes klart ud. Kun derved kan Folketinget foretage den nødvendige proportionalitetsvurdering.

Anbefalinger

- **Indhent dokumentation:** Kræv oversigter over brud på §§114–114j samt for organiseret kriminalitet og spionage de seneste 25 år som grundlag for at vurdere base-rate-problemet og manglen på træningsdata.

- **Gennemfør teknisk vurdering:** Kræv en uafhængig evaluering af PET's planlagte AI-system og dokumentation for systemets faktiske egnethed, før loven kan behandles videre.

- **Ved uegnethed:** Indfør målrettede alternativer baseret på konkret mistanke og dommerkendelse.

- **Ved egnethed og proportionalitet:** Fastlæg i loven, hvilke datakategorier PET kan indhente, og undtag eksplicit sundhedsoplysninger – herunder genetiske og psykiatriske data.

Hvis Folketinget alligevel ønsker at give PET nye analytiske værktøjer, bør man først undersøge privacy-bevarende alternativer som beskrevet i Bilag B**,** hvor moderne kryptografiske teknikker kan forene sikkerhedsbehov med respekt for borgernes privatliv.

Mvh

Praktiserende læge Thomas Birk Kristiansen

Referencer

1. Folketinget. L 218: Forslag til lov om ændring af lov om Politiets Efterretningstjeneste (data- og analysebaseret efterretningsvirksomhed m.v.). Fremsat 25. april 2025. 2024-25 samling.https://www.ft.dk/samling/20241/lovforslag/l218/index.htm
2. Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger (GDPR), artikel 2, stk. 2, litra a.
3. Databeskyttelsesloven. Lov nr. 502 af 23. maj 2018, § 3, stk. 2.
4. EU-Domstolen. Digital Rights Ireland Ltd mod Minister for Communications m.fl. Forenede sager C-293/12 og C-594/12. Dom af 8. april 2014.
5. EU-Domstolen. La Quadrature du Net m.fl. mod Premier ministre m.fl. Forenede sager C-511/18, C-512/18 og C-520/18. Dom af 6. oktober 2020.
6. Hummelgaard P. Svar på spørgsmål 55 til L 218. København: Justitsministeriet; 2025 aug 27. [citeret 2025 nov 20]. Tilgængelig fra: https://www.ft.dk/samling/20241/lovforslag/L218/spm/55/svar/2157358/3059009.pdf
7. Den tværministerielle indsatsgruppe ("Bjelkegruppen"). Indsatsen over for terrordømte og radikaliserede indsatte under varetægt og afsoning. Rapport 1 - Før løsladelse. København: Justitsministeriet; 2021 sep. https://www.justitsministeriet.dk/wp-content/uploads/2021/10/Indsatsen-over-for-terrordoemte-og-radikaliserede-indsatte-under-varetaegt-og-afsoning.pdf
8. PET. Årlig redegørelse 2022. København: Politiets Efterretningstjeneste; 2023.
9. Straffelovrådet. Betænkning nr. 1581 om strafudmåling. København: Justitsministeriet; 2023.
10. Folketingets Retsudvalg. *Beretning om terrorangrebet i København den 14. og 15. februar 2015.* København: Folketinget; 2015. (2014/1 BR 7).
11. He H, Garcia EA. Learning from imbalanced data. IEEE Trans Knowl Data Eng. 2009;21(9):1263-84.
12. Gigerenzer G, Gaissmaier W, Kurz-Milcke E, Schwartz LM, Woloshin S. Helping doctors and patients make sense of health statistics. Psychol Sci Public Interest. 2007;8(2):53-96.
13. Colquhoun D. An investigation of the false discovery rate and the misinterpretation of p-values. R Soc Open Sci. 2014;1(3):140216.
14. Yoon JH, Strand F, Baltzer PAT, et al. Standalone AI for breast cancer detection at screening DM/DBT: systematic review and meta-analysis. Radiology. 2023;307(5):e222639. doi:10.1148/radiol.222639.
15. Hernström V, Josefsson V, Sartor H, Schmidt D, Larsson AM, Hofvind S, Andersson I, Rosso A, Hagberg O, Lång K. Screening performance and characteristics of breast cancer detected in the Mammography Screening with Artificial Intelligence trial (MASAI): a randomised, controlled, parallel-group, non-inferiority, single-blinded, screening accuracy study. Lancet Digit Health. 2025 Mar;7(3):e175-e183. doi: 10.1016/S2589-7500(24)00267-X. Epub 2025 Feb 3. PMID: 39904652.
16. Danish Comprehensive Cancer Center. Klinisk anvendelse af kunstig intelligens på kræftområdet: Muligheder og barrierer for national udbredelse. Grau C, Bøgsted M, redaktører. Aarhus: DCCC; 2024 mar 4. Tilgængelig fra: https://www.dccc.dk/siteassets/fokusomrader/klinisk-anvendelse-af-kunstig-intelligens/dcccklinisk-anvendelse-af-kunstig-intelligens-pa-kraftomradet.pdf
17. Hastie T, Tibshirani R, Friedman J. *The elements of statistical learning: data mining, inference, and prediction*. 2nd ed. New York: Springer; 2009.
18. Bishop CM. Pattern recognition and machine learning. New York: Springer; 2006.
19. Duda RO, Hart PE. *Pattern Classification and Scene Analysis*. New York: Wiley; 1973.
20. Bellman RE. Dynamic programming. Princeton: Princeton University Press; 1957.
21. Hughes GF. On the mean accuracy of statistical pattern recognizers. IEEE Trans Inf Theory. 1968;14(1):55-63.
22. D'Amour A, Heller K, Moldovan D, Adlam B, Alipanahi B, Beutel A, et al. Underspecification presents challenges for credibility in modern machine learning. J Mach Learn Res. 2022;23(226):1-61.

23. National Institute of Standards and Technology (NIST). AI Risk Management Framework 1.0 (AI 100-1). Gaithersburg, MD: U.S. Department of Commerce; 2023.
24. Kristiansen TB, Kristensen K, Uffelmann J, Brandslund I. Erroneous data: The Achilles' heel of AI and personalized medicine. Front Digit Health. 2022;4:862095.
25. Sambasivan N, Kapania S, Highfill H, Akrong D, Paritosh P, Aroyo L. "Everyone wants to do the model work, not the data work": Data cascades in high-stakes AI. In: CHI '21. New York: ACM; 2021. s.1-15.
26. Wang RY, Strong DM. Beyond accuracy: What data quality means to data consumers. Journal of Management Information Systems. 1996;12(4):5-33.
27. Rigsadvokaten. Orientering om teledata. København: Rigsadvokaten; 2019 jul 8.
28. Justitsministeriet. Redegørelse om brug af teledata i straffesager. København: Justitsministeriet; 2020.
29. Politiken. Telefejl er værre end antaget: Mastedata kan være fejlmålt med op mod 100 kilometer. 2019 sep 26.
30. Greibe T. Fejlkodning af diabetes II og datafangst. Månedsskr Prakt Lægegern. 2014;92(5):375-8.
31. Nielsen AA, Christensen H, Lund ED, et al. Diabetes mortality differs between registers due to various disease definitions. Dan Med J. 2014;61(5):A4840.
32. Ellesøe SG, Jensen AB, Ängquist LH, et al. Validation of diagnoses on 1,593 families with congenital heart disease. World J Pediatr Congenit Heart Surg. 2016;7(2):169-77.
33. Folketingets Ombudsmand. Foreløbige ejendomsvurderinger af ejerboliger (FOB 2024-10). København; 2024 apr 3. Sagsnr. 23/04884.
34. DR Nyheder. 190.000 tilstandsrapporter modsiger minister: BBR er smækfyldt med fejl. 2023 mar 21.
35. Skatteministeriet. Orientering til Folketingets Skatteudvalg om status for Ejendom & Grund (E&G) - projektudgifter 2014-2025. SAU, Alm.del, bilag 258; 2025 jun 20.
36. Fazel S, et al. Prediction of violent reoffending using risk assessment instruments in individuals with criminal convictions: systematic review and meta-analysis. BMJ. 2022;378:e070769.
37. Dressel J, Farid H. The accuracy, fairness, and limits of predicting recidivism. Science Advances. 2018;4(1):eaao5580.
38. Prins SJ, Reich A. Criminogenic risk assessment: A meta-review and critical analysis. Punishm Soc. 2021;23(4):578-604. doi:10.1177/14624745211025751
39. Ly D. Predictive policing: myth busting and what we can expect of AI-powered law enforcement. Forbes. 2024 Oct 15 [citeret 2025 nov 20]. Tilgængelig fra: https://www.forbes.com/councils/forbestechcouncil/2024/10/15/predictive-policing-myth-busting-and-what-we-can-expect-of-ai-powered-law-enforcement/
40. Diderichsen A. Masseovervågning i ny PET-lov giver ikke mere sikkerhed. Politiken. 2025 apr 26. Tilgængelig fra: https://politiken.dk/debat/kroniken/art10382716/Masseovervågning-i-ny-PET-lov-giver-ikke-mere-sikkerhed
41. Vigild DJ. Han forsker i kunstig intelligens: Ny PET-lov vil ikke kunne forudsige terror med ai. Berlingske. 2025 aug 28. Tilgængelig fra: https://www.berlingske.dk/synspunkter/han-forsker-i-kunstig-intelligens-ny-pet-lov-vil-ikke-kunne-forudsige-terror-med-ai
42. Verhelst HM, Stannat AW, Mecacci G. Machine learning against terrorism: How big data collection and analysis influences the privacy-security dilemma. Sci Eng Ethics. 2020;26(6):2975-84. https://link.springer.com/article/10.1007/s11948-020-00254-w
43. Agaku IT, Adisa AO, Ayo-Yusuf OA, Connolly GN. Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. J Am Med Inform Assoc. 2014;21(2):374-8.
44. Mendelson TB, Ravitsky V, Dumez B, Schuster T, Godard B, Birko S, et al. Public views on sharing anonymised patient-level data where there is a mixed public and private benefit. BMC Med Ethics. 2022;23:10.

45. Ploug T, Holm S. Informed consent and routinisation. J Med Ethics. 2013;39(4):214-8.
46. Kristensen DB, Askegaard S, Jespersen LK. The ambiguous politics of digital health data: Privacy, data sharing and trust. Soc Sci Med. 2021;290:114372.
47. Sarma KM, Carthy SL, Cox KM. Mental disorder, psychological problems and terrorist behaviour: a systematic review and meta-analysis. Campbell Syst Rev. 2022;18(3):e1268.
48. Den Europæiske Menneskerettighedskonvention, artikel 14 (Forbud mod diskrimination).
49. FN's konvention om rettigheder for personer med handicap (Convention on the Rights of Persons with Disabilities, CRPD) fra 2006, som Danmark ratificerede i 2009.
50. Sundhedsloven, LBK nr. 210 af 27/01/2022, § 223 b, stk. 2.
51. Retshåndhævelsesloven, LBK nr. 1148 af 11/10/2017, § 10.
52. Nationalt Genom Center. Årsrapport 2024 - Status pr. 31. december 2024.
53. Indenrigs- og Sundhedsministeriet & Danske Regioner. Analyse af et nationalt strategisk initiativ for biobankinfrastrukturen i Danmark. Januar 2025.
54. iPSYCH. Guidelines for iPSYCH partition at the GenomeDK HPC cluster. Aarhus University; 2021.
55. Inampudi A. Blood taken from Danish babies ended up in huge genetic study—without consent. Science. 2025 aug 1;389(6760):974-975.
56. Gudbjartsson DF, Helgason H, Gudjonsson SA, Zink F, Oddson A, Gylfason A, Besenbacher S, Magnusson G, Halldorsson BV, Hjartarson E, Sigurdsson GT, Stacey SN, Frigge ML, Holm H, Saemundsdottir J, Helgadottir HT, Johannsdottir H, Sigfusson G, Thorgeirsson G, Sverrisson JT, Gretarsdottir S, Walters GB, Rafnar T, Thjodleifsson B, Bjornsson ES, Olafsson S, Thorarinsdottir H, Steingrimsdottir T, Gudmundsdottir TS, Theodors A, Jonasson JG, Sigurdsson A, Bjornsdottir G, Jonsson JJ, Thorarensen O, Ludvigsson P, Gudbjartsson H, Eyjolfsson GI, Sigurdardottir O, Olafsson I, Arnar DO, Magnusson OT, Kong A, Masson G, Thorsteinsdottir U, Helgason A, Sulem P, Stefansson K. Large-scale whole-genome sequencing of the Icelandic population. Nat Genet. 2015 May;47(5):435-44. doi: 10.1038/ng.3247. Epub 2015 Mar 25. PMID: 25807286.
57. Koops BJ. The concept of function creep. Law Innov Technol. 2021;13(1):29-56.
58. Dahl JY, Sætnan AR. "It all happened so slowly" – On controlling function creep in forensic DNA databases. Int J Law Crime Justice. 2009;37(3):83-103.
59. Justitsministeriet. Rapport om erfaringerne med PET-loven. København: Justitsministeriet; 2022.

Bilag A – Aktindsigt fra Justitsministeriet

Dokumentliste vedrørende L 218, fremsøgt med søgeordene *"genetisk"* og *"genetiske"*. Dette viser, at genetiske oplysninger eksplicit indgik i ministeriets egen sagsforberedelse af L 218 i perioden 2022-2025. Jeg har ikke endnu fået indsigt i de enkelte dokumenter.

Bilag B: Privacy-bevarende teknologier som alternativ til masseovervågning

Muligheden for anonymiseret dataanalyse under domstolskontrol

Som alternativ til den foreslåede model i L218 bør Folketinget overveje en arkitektur baseret på privacy-bevarende teknologier, der muliggør indledende analyse på anonymiserede data – kombineret med domstolskontrol før eventuel identifikation af enkeltpersoner. Denne model sikrer, at sikkerhedsbehov kan imødekommes uden at krænke borgernes grundlæggende rettigheder.

Teknisk løsningsmodel

Moderne kryptografiske teknikker som Multi-party Computation (MPC) [1], homomorf kryptering [2] og differential privacy [3] gør det muligt at analysere data uden at afsløre individuelle identiteter. Under en sådan model kunne PET arbejde i tre faser:

Fase 1 – Anonymiseret screening: AI-algoritmer anvendes på krypterede eller anonymiserede datasæt for at identificere mønstre, der kan indikere sikkerhedstrusler. Identiteter forbliver skjulte gennem hele analyseprocessen via kryptografisk beskyttelse.

Fase 2 – Domstolsprøvelse: Kun hvis analysen peger på reelle og konkrete trusler må PET indhente dommerkendelse for at de-anonymisere og undersøge specifikke individer. Dette kunne implementeres via en særlig domstol for sikkerheds- og efterretningsanliggender.

Fase 3 – Målrettet efterforskning: Med dommerkendelse kan PET anvende traditionelle efterforskningsmetoder over for de konkret identificerede individer.

Fordele ved modellen

- **Proportionalitet:** Indledende analyser berører ikke privatlivet for den brede befolkning
- **Retssikkerhed:** Identifikation af borgere sker først efter uafhængig domstolskontrol
- **Teknisk gennemførlighed:** MPC anvendes allerede praktisk [4-7]
- **Transparens:** Zero-knowledge-proofs muliggør systemaudit uden at kompromittere operationelle metoder [8].
- **Beskyttelse af uskyldige:** Kun personer vurderet relevante af domstol identificeres.
- **Økonomi:** Ved at begrænse manuel efterforskning til de få tilfælde, hvor en domstol har givet tilladelse, kan PET undgå at spilde ressourcer på hundredtusindvis af falske positiver og dermed opnå betydelige effektiviseringsgevinster.

Begrænsninger og risici

- **Base-rate-problemet:** Modellen eliminerer ikke det underliggende statistiske problem med falske positiver beskrevet i hoveddokumentet, men den reducerer markant antallet af uskyldige borgere, hvis data eksponeres.

- **Teknisk kompleksitet:** Implementering kræver betydelig ekspertise. Dog viser erfaringer fra Alexandra Instituttet med FRESCO-frameworket, at dansk ekspertise allerede findes [7].

- **Function creep:** Selv privacy-bevarende systemer kan udvides over tid. Derfor kræves:
    - Lovgivningsmæssige grænser for analysetyper
    - Uafhængige revisioner hvert halve år
    - Offentlig rapportering om systemets anvendelse og fejlrate
    - Løbende solnedgangsklausul, der kræver fornyet parlamentarisk godkendelse efter 3 år

Anbefaling

Folketinget kan overveje at pålægge Justitsministeriet at undersøge den tekniske og juridiske gennemførlighed af privacy-bevarende alternativer inden L218 vedtages. En sådan undersøgelse kan involvere danske eksperter fra Alexandra Instituttet, IT-Universitetet og DTU, samt internationale erfaringer fra sammenlignelige demokratier.

Dette kan forene legitime sikkerhedsbehov med beskyttelsen af borgernes grundlæggende rettigheder og dermed undgå den masseovervågning som L218 i sin nuværende form lægger op til.

Pilotordning

En pilotordning kunne iværksættes på et afgrænset område, så tekniske og juridiske udfordringer identificeres og adresseres, før en eventuel bredere implementering. Dette vil give Folketinget et reelt grundlag at træffe beslutning på – i stedet for at vedtage en lov, der i praksis risikerer at indføre masseovervågning uden effekt.

Referencer til bilag B

1. Yao AC. Protocols for secure computations. 23rd Annual Symposium on Foundations of Computer Science. IEEE; 1982. p. 160-164.
2. Gentry C. Fully homomorphic encryption using ideal lattices. Proceedings of the 41st annual ACM symposium on Theory of computing. 2009. p. 169-178.
3. Dwork C, Roth A. The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science. 2014;9(3-4):211-407.
4. Cho H, Wu DJ, Berger B. Secure genome-wide association analysis using multiparty computation. Nature Biotechnology. 2018;36(6):547-551.
5. Bogdanov D, Jõemets M, Siim S, Vaht M. How the Estonian Tax and Customs Board Evaluated a Tax Fraud Detection System Based on Secure Multi-party Computation. Financial Cryptography and Data Security. Springer; 2015. p. 227-234.
6. Kamm L, Bogdanov D, Laur S, Vilo J. A new way to protect privacy in large-scale genome-wide association studies. Bioinformatics. 2013;29(7):886-893.
7. Damgård I, Keller M, Larraia E, Pastro V, Scholl P, Smart NP. Practical covertly secure MPC for dishonest majority – Or: Breaking the SPDZ limits. European Symposium on Research in Computer Security. Springer; 2013. p. 1-18
8. Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof systems. SIAM Journal on Computing. 1989;18(1):186-208.

Bilag C: Digital infrastruktur for PET's AI-anvendelse bør være under dansk kontrol

Lovforslaget forudsætter, at PET kan indsamle og analysere store datasæt ved hjælp af kunstig intelligens på high performance computing-anlæg (HPC). Dette rejser spørgsmålet om valg af infrastruktur, hvor Gefion og Computerome er de mest oplagte kandidater. Valget er ikke kun teknisk, men i høj grad sikkerhedsmæssigt.

Juridiske og sikkerhedsmæssige udfordringer ved Gefion

Gefion blev lanceret i oktober 2024 som en del af Danish Centre for AI Innovation [1-3] og hostes af Digital Realty, et amerikansk datacenterselskab [4]. Dette rejser en væsentlige problematik:

- **CLOUD Act-eksponering**: USA's *CLOUD Act* (Clarifying Lawful Overseas Use of Data Act, 2018) giver amerikanske myndigheder ret til at kræve data udleveret fra amerikanske virksomheder – uanset hvor i verden data fysisk befinder sig. Både European Data Protection Board og European Data Protection Supervisor har påpeget alvorlige problemer i forhold til europæisk databeskyttelse [5,6]. I *Schrems II*-dommen fra juli 2020 fastslog EU-Domstolen, at amerikanske overvågningsprogrammer ikke yder EU-borgere et beskyttelsesniveau, der svarer til det, der garanteres i EU [7]. Dette gør placering af særligt følsomme data på amerikansk-kontrolleret infrastruktur både juridisk og sikkerhedsmæssigt problematisk.

Tekniske kapaciteter i kontekst

Gefion, baseret på NVIDIA's DGX SuperPOD-teknologi, repræsenterer nyeste generation af AI-optimeret hardware. Computerome [8] har siden 2019 fungeret som national HPC-installation og håndteret Danmarks mest krævende forskningsopgaver, herunder omfattende genomisk analyse og sundhedsdata.

For PET's analytiske formål er begge platforme teknisk kapable. Den afgørende forskel ligger i jurisdiktion: Computerome opererer under fuld dansk jurisdiktion på DTU's område, mens Gefion gennem Digital Realty er underlagt amerikansk selskabsret og dermed *CLOUD Act*.

Konklusion

Der opstår et grundlæggende paradoks, hvis PET – som har ansvar for at beskytte Danmark mod udenlandsk efterretning – placerer sine mest følsomme analyser på en infrastruktur underlagt amerikansk jurisdiktion og potentielt tilgængelig for udenlandske myndigheder gennem *CLOUD Act*.

Hvis PET gennem L218 får adgang til "større sammenhængende datasæt", bør det fastslås, at særligt følsomme analyser – især dem der involverer genetiske data, sundhedsoplysninger eller omfattende personprofiler – skal processeres på infrastruktur under fuld dansk jurisdiktion og kontrol.

Dette peger på Computerome som den mest hensigtsmæssige platform for PET's mest sensitive AI-analyser.

Referencer til bilag C

1. NVIDIA Corporation. *NVIDIA and Novo Nordisk Foundation launch Denmark's Gefion AI supercomputer.*https://nvidianews.nvidia.com/news/nvidia-novo-nordisk-foundation-launch-denmarks-gefion

2. Novo Nordisk Foundation. *Denmark launches national AI supercomputer Gefion.*https://novonordiskfonden.dk/en/news/denmarks-first-ai-supercomputer-is-now-operational/
3. NVIDIA. *Gefion: Denmark's new AI supercomputer powered by NVIDIA DGX SuperPOD.*https://blogs.nvidia.com/blog/denmark-sovereign-ai-supercomputer/
4. Digital Realty. *Digital Realty to host Denmark's national AI supercomputer Gefion.*https://www.digitalrealty.com/about/newsroom/press-releases/123257/digital-realty-to-host-nvidia-powered-ai-supercomputer-in-denmark
5. European Data Protection Board; European Data Protection Supervisor. *Joint response to the LIBE Committee on the impact of the US CLOUD Act on the European legal framework for personal data protection.* Bruxelles: EDPB/EDPS; 2019 Jul 10.
6. European Data Protection Supervisor. *The CLOUD Act: Implications for EU data protection law.* Opinion 5/2019. 2019.
7. Court of Justice of the European Union. *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (C-311/18) (Schrems II).* Dom af 2020 Jul 16. ECLI:EU:C:2020:559.
8. Danmarks Tekniske Universitet. *Computerome – National Life Science Supercomputing Center.*https://computerome.dk