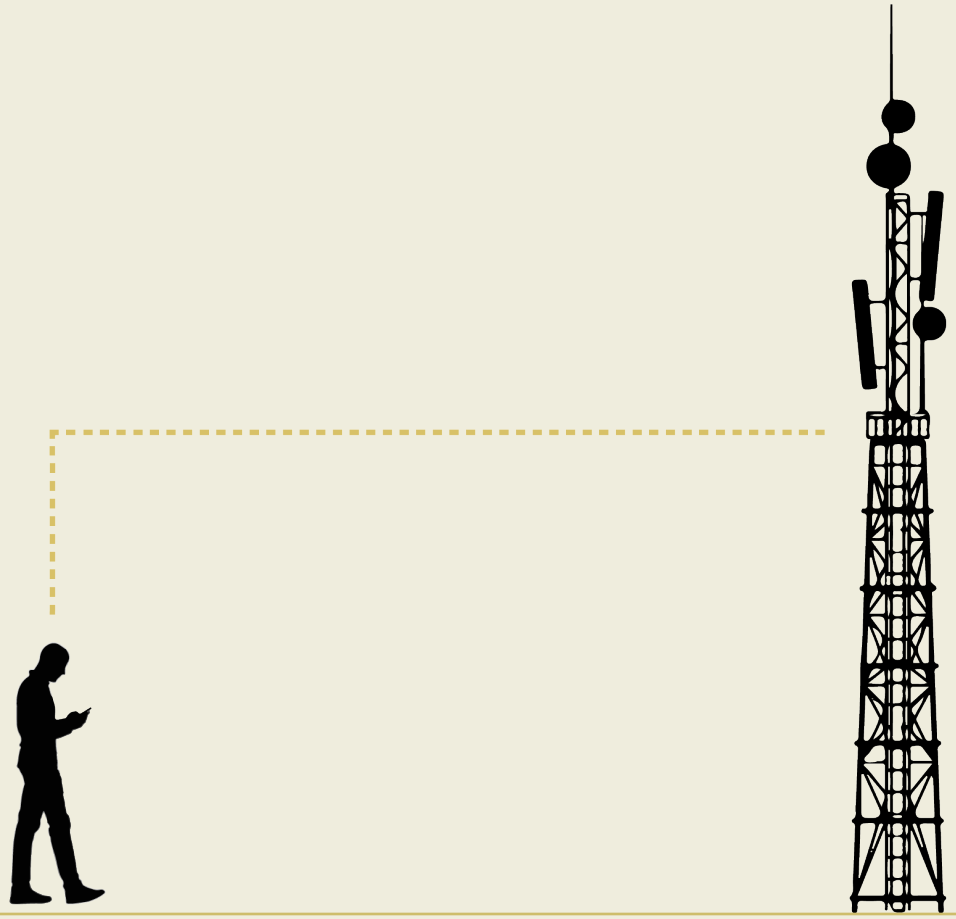
JUSTITIA

DANMARKS UAFHÆNGIGE
JURIDISKE TÆNKETANK



Sammenfatning:

ULOVLIG LOGNING – TID TIL EN LOVREVISION

Af Jacob Mchangama og Helene Qvist Petersen

Revision af logningsreglerne – Sammenfatning

Indledning

Terrorangrebene i USA den 11. september 2001 medførte et paradigmeskifte i vestlige demokratiers vilje til at overvåge deres borgere. Som en følge af anti-terrorindsatsen fra 2002 trådte de danske logningsregler i kraft i 2007. Med logningsreglerne blev teleselskaberne forpligtet til at indsamle og opbevare en lang række oplysninger om samtlige danskeres elektroniske kommunikation. De oplysninger, der skal logges, omfatter bl.a. hvem borgerne SMS'er med og ringer til, hvornår og hvor længe de gør det, samt hvor de opholder sig, når de foretager denne kommunikation. Oplysningerne gør det muligt at lave en meget præcis profil over hver enkelt persons adfærd. Indholdet i kommunikationen skal ikke registreres.

Reglerne har siden været genstand for omfattende debat, og selvom Justitsministeriet i fire år har anerkendt, at de nuværende regler strider mod EU-retten, er de endnu ikke blevet ændret.

Justitia argumenterer i denne analyse for, at de nuværende regler må anses for ugyldige, og at teleselskaberne hverken skal eller bør foretage logning, før der er vedtaget nye, lovlige logningsregler. Justitia kommer i den forbindelse med en række konkrete anbefalinger til nye logningsregler.

Logningsreglerne strider mod EU-retten men opretholdes fortsat

Logning er gentagne gange i årenes løb blevet fremhævet som et afgørende redskab for politiet i forbindelse med sager om bl.a. terrorisme, organiseret narkohandel, drab, bandekriminalitet og databedrageri.

Sideløbende har det i en lang årrække været omdiskuteret, i hvilket omfang logning er i overensstemmelse med grundlæggende rettigheder som retten til privatliv, beskyttelsen af personoplysninger og ytringsfriheden. EU-Domstolens praksis har – som minimum – siden 2016 gjort det klart, at de danske logningsregler er i strid med disse rettigheder.

Ved tre domme fra 2014, 2016 og 2020 har EU-domstolen således fastslået, at 1) EU's logningsdirektiv, som de danske regler bygger på, er ugyldigt, 2) at EU-retten ikke tillader national lovgivning, der kræver generel og udifferentieret logning af samtlige trafik- og lokaliseringsdata, og 3) at en national domstol ikke kan opretholde nationale logningsregler midlertidigt, når de strider mod EU-retten.

EU-Domstolen åbner dog for, at der lovligt kan ske *målrettet* logning til bekæmpelse af (som minimum) grov kriminalitet, og at generel og udifferentieret logning kan ske midlertidigt, hvis en

Justitia | Fruebjergvej 3 | 2100 København Ø | 23926100 | info@justitia-int.org

medlemsstat står overfor en alvorlig trussel mod den nationale sikkerhed, der er "reel og aktuel eller forudsigelig" (f.eks. en konkret terrortrussel).

Den danske regering har for så vidt anerkendt, at de danske logningsregler strider mod EU-retten, idet Justitsministeriet gentagne gange har bekræftet, at dommene fra 2016 og 2020 giver anledning til at ændre de danske regler.

Ikke desto mindre er reglerne fortsat uændrede. I de seneste fire år har regeringens primære begrundelse for at udskyde lovrevisionen været, at man har måttet afvente retningslinjer fra EU samt dialog med de øvrige medlemsstater. Senest tilkendegav Justitsministeriet i januar 2021, at lovrevisionen heller ikke kunne forventes at ske i februar 2021, hvilket ellers var planen.

Justitsministeriet har løbende anført, at tilpasning af logningsreglerne blot skal ske "hurtigst muligt", hvorefter de nuværende regler kan opretholdes, indtil tilpasningen er sket. Dette er Justitia ikke enig i. Som anført følger det direkte af La Quadrature-dommen, at logningsregler, der strider mod EU-retten, ikke kan håndhæves af en national domstol. Når det er afklaret, at en given lovgivning ikke kan håndhæves af en domstol, må dette også betyde, at den pågældende lovgivning må anses ugyldig og ikke kan opretholdes. Dette er med andre ord, ifølge Justitias vurdering, to sider af samme sag.

Justitsminister Nick Hækkerup har da også anerkendt, at logningsreglerne ikke længere kan håndhæves overfor teleselskaberne. Dette må anses som et skridt i den rigtige retning. Dog mener ministeren samtidig, at reglerne fortsat er gyldige og "i kraft", og opfordrer telebranchen til at efterleve de klart ulovlige logningsregler.

Dette fremstår svært problematisk. Justitia finder det svært at forstå, hvordan regler, der ikke kan håndhæves, fortsat kan siges at være i kraft. Ifølge Justitias opfattelse modsiger disse to udmeldinger hinanden.

Betænkelighederne ved den fortsatte opretholdelse af de EU-retsstridige regler skærpes yderligere ved, at der er tale om et intensivt og konstant indgreb i grundlæggende rettigheder for praktisk talt hele Danmarks befolkning. De danske sager om fejl i konverteringen af loggede data og udlevering af for mange oplysninger til politiet viser også, at bekymringer vedrørende logning ikke blot er teoretiske frygtscenarier eller "juristeri".

Justitsministerens opfordring til efterlevelse af logningsreglerne er så meget desto mere problematisk, fordi teleselskaberne, hvis de efterlever opfordringen, risikerer at blive retsforfulgt for at overtræde persondataretten.

Både Teleindustrien og Retsudvalget har spurgt justitsministeren, om det vil være i overensstemmelse med databeskyttelsesreglerne, hvis teleselskaberne fortsætter med at logge som hidtil. Hertil har ministeren svaret, at "*Efter GDPR vil der fortsat kunne logges trafik- og*

Justitia | Fruebjergvej 3 | 2100 København Ø | 23926100 | info@justitia-int.org

lokaliseringsdata som hidtil med henblik på beskyttelse af national sikkerhed og bekæmpelse af grov kriminalitet" (Justitias understregning).[1]

Retorikken i ministerens svar – at der "fortsat" kan "logges som hidtil" – giver anledning til at forstå svaret sådan, at logning kan fortsætte uændret og samtidig overholde databeskyttelsesreglerne. Svaret indeholder imidlertid også en præmis om, at logning kun er i overensstemmelse med databeskyttelsesreglerne, når det sker af hensyn til to specifikke formål: National sikkerhed og grov kriminalitet.

Med det nuværende retlige landskab er det imidlertid ikke praktisk muligt for teleselskaberne at afgrænse logningen til beskyttelse af national sikkerhed og bekæmpelse af grov kriminalitet. Det er derfor også svært at se, hvordan selskaberne skal kunne logge inden for rammerne af databeskyttelsesreglerne, hvis de fortsat logger. Dette glemmer justitsministeren at nævne i sit svar til Teleindustrien, hvilket Justitia finder kritisabelt.

Justitia mener hverken, at telebranchen skal eller bør efterleve reglerne i den nuværende logningsbekendtgørelse. Justitia anerkender dog, at logning og adgang til dataene udgør et vigtigt redskab i politi og efterretningstjenesters arbejde med at forhindre og opklare alvorlig kriminalitet. Derfor anbefales i stedet følgende løsninger:

Anbefalinger

Nedenstående er en kort sammenfatning af hovedpointerne i Justitias anbefalinger. Se den fulde analyse for de nærmere detaljer.

Midlertidig løsning indtil vedtagelsen af nye, lovlige logningsregler:

Justitia anbefaler, at der indføres en midlertidig løsning, der respekterer grundlæggende rettigheder, samtidig med at myndighederne ikke helt fratages logningsredskabet i den mellemliggende periode. Der kunne her opereres med en løsning, hvor data først logges, når der er opstået mistanke mod en person, eventuelt ud fra et lempet mistankekrav. Retsplejeloven tillader allerede i dag en lignende form for hastesikring af data, men Justitias forslag vil give videre muligheder herfor.

Anbefalinger til nye logningsregler i overensstemmelse med EU-Domstolens praksis:

Justitia anbefaler, at der i overensstemmelse med EU-Domstolens praksis laves særskilte løsninger for logning af henholdsvis 1) trafik- og lokaliseringsdata, 2) IP-adresser og 3) brugeridentitetsoplysninger.

[1] Citatet er taget fra justitsministerens besvarelse til Teleindustrien. Besvarelsen til Retsudvalget er ikke ordret identisk hermed, men de to besvarelser svarer indholdsmæssigt til hinanden

Justitia | Fruebjergvej 3 | 2100 København Ø | 23926100 | info@justitia-int.org

MULIGHED FOR LOGNING
(under iagttagelse af nærmere bestemte betingelser – ikke uddybet her)

Trafik- og lokaliseringsdata	Alvorlig trussel mod den nationale sikkerhed	Alvorlig trussel mod den offentlige sikkerhed/grov kriminalitet	Kriminalitet i almindelighed
Generel og udifferentieret	✓	✗	✗
Målrettet	✓	✓	✗
IP-adresser	✓	✓	✗
Brugeridentitetsoplysninger	✓	✓	✓

1) Logning af trafik og lokaliseringsdata

Trafikdata omfatter bl.a. afsendelse/modtagelse af SMS'er og telefonopkald. *Lokaliseringsdata* omfatter bl.a. mastedata, dvs. oplysninger om hvor en person befinder sig, når vedkommende kommunikerer via f.eks. sin mobiltelefon.

Omfanget af logning af disse data afhænger af, til hvilket formål dataene logges. Der bør derfor opereres med to særskilte løsninger: 1.1) målrettet logning til bekæmpelse af som minimum grov kriminalitet og 1.2) generel og udifferentieret logning til beskyttelse af alvorlige trusler mod den nationale sikkerhed.

1.1) Målrettet logning af trafik- og lokaliseringsdata til bekæmpelse af som minimum grov kriminalitet

- Målrettet logning kan ske til bekæmpelse af *grov kriminalitet*, beskyttelse mod *alvorlige trusler mod den offentlige* sikkerhed samt beskyttelse mod trusler generelt mod den *nationale sikkerhed*. De nye logningsregler skal derfor først og fremmest definere disse tre begreber
- Logningen skal målrettes med hensyn til 1) kategorierne af data, 2) de omhandlede kommunikationsmidler, 3) de berørte personer, og 4) den fastsatte varighed af lagringen.
- Ordningen bør være dynamisk, så der løbende kan udstedes konkret afgrænsede påbud om logning
- Et logningspåbud skal være baseret på en konkret vurdering af, hvad der på et givent tidspunkt udgør strengt nødvendig logning til bekæmpelse af f.eks. grov kriminalitet
    - Det indledende skridt i en sådan konkret vurdering bør være identificeringen af en konkret begivenhed, der kan begrunde logning (f.eks. grov menneskehandel).

Justitia | Fruebjergvej 3 | 2100 København Ø | 23926100 | info@justitia-int.org

- Den nærmere afgrænsning af logningen kan herefter tage sit udgangspunkt i kriteriet "de berørte personer", dvs. den personmæssige afgrænsning
  - Den personmæssige afgrænsning kan både ske med hensyn til specifikke personer, til hvem der er knyttet en mistanke, og geografisk, således at data tilhørende de personer, der befinder sig i nærmere bestemte områder, logges
  - Der kan i den forbindelse opereres med lempede mistankekrav
- Den efterfølgende afgrænsning med hensyn til kategorierne af data og de omhandlede kommunikationsmidler kan basere sig på et grundprincip om, at jo mere snævert den personmæssige logning er afgrænset, jo bredere kan de omfattede kommunikationsmidler og kategorier af data afgrænses
- Logningspåbuddet, dvs. påbuddet om selve indsamlingen af data, bør også være tidsbegrænset. Her kan der opereres med et udgangspunkt på f.eks. tre måneder med mulighed for både forlængelse og afkortning

Målrettet logning af trafik- og lokaliseringsdata

Et logningspåbud skal baseres på en konkret vurdering af, hvad der på et givent tidspunkt udgør strengt nødvendig logning til bekæmpelse af f.eks. grov kriminalitet

1. **Identifikation**
   Identificering af en begivenhed som kræver logning.
2. **Afgrænsning af de berørte personer**
   Afgrænsningen kan både ske mht. specifikke personer og/eller geografisk (så data tilhørende personer, der befinder sig et givent sted, logges).
   Der kan opereres med lempede mistankekrav.
3. **Afgræsning af datakategorier og kommunikationsmidler**
   Afgrænses ud fra følgende princip: Jo snævrere personmæssig afgrænsning, jo brede kan datakategorier og kommunikationsmidler afgrænses.
4. **Tidsmæssig afgrænsning**
   Logningspåbud bør altid være tidsbegrænset. Der kan opereres med et udgangspunkt på f.eks. tre måneder med mulighed for både forlængelse og afkortning

2) Generel og udifferentieret logning til beskyttelse af alvorlige trusler mod den nationale sikkerhed

- Generel og udifferentieret logning kan – i snævre tilfælde – iværksættes til beskyttelse mod en alvorlig trussel mod den nationale sikkerhed, som er "reel og aktuel eller forudsigelig".
- Loven skal definere begrebet "*alvorlig* trussel mod den nationale sikkerhed".
- Loven skal indeholde parametre til brug for vurderingen af, om der er tale om en reel og aktuel eller forudsigelig trussel. Der skal være krav om konkrete, dokumenterbare omstændigheder. En abstrakt terrorrisiko ud fra det generelle trusselsbillede må ikke være tilstrækkelig.
- Selve indsamlingen af data skal være midlertidig, og logningspåbuddet skal derfor være tidsbegrænset. Her kan der opereres med et udgangspunkt på f.eks. 14 dage med

Justitia | Fruebjergvej 3 | 2100 København Ø | 23926100 | info@justitia-int.org

mulighed for både forlængelse og afkortning samt pligt til løbende stillingtagen til det konkrete trusselsbillede
- Iværksættelse af generel og udifferentieret logning bør kun kunne ske efter kendelse fra byretten

2) Logning af IP-adresser

En *IP-adresse* er en kode, der tildeles en kommunikationsenhed (f.eks. en computer), når den tilkobles internettet. Koden er knyttet til det netværk, enheden kobles på, og flere enheder koblet på samme netværk tildeles derfor den samme IP-adresse.

- Der kan ske generel og udifferentieret logning af IP-adresser
- Adgangen til disse data skal begrænses til bekæmpelse af som minimum *grov* kriminalitet

3) Logning af brugeridentitetsoplysninger

Brugeridentitetsoplysninger er – som ordet foreskriver – oplysninger om identiteten på den person, der har tegnet et abonnement, f.eks. navn og adresse på en teleabonnent.

- Der kan ske logning for samtlige brugere af elektroniske kommunikationsmidler
- Adgang til disse data skal være begrænset til bekæmpelse af kriminalitet i almindelighed

Justitia | Fruebjergvej 3 | 2100 København Ø | 23926100 | info@justitia-int.org