INSPIRATIONSMATERIALE

Overvågning og sikkerhed

Information

Information

KR. 20,00 €2,66 UAFHÆNGIG AF PARTIPOLITISKE OG ØKONOMISKE INTERESSER TORSDAG 19. JUNI 2014

(TS//SI//REL TO USA, DNK) Emphasize NSA's commitment to the special access and assisting DDIS in managing the access.

Remind the Danes of the long NSA-DDIS partnership working cable access with.

Note that we look forward to new areas of cooperation.

Et talepapir fra 2012 til daværende NSA-chef Keith Alexander viser, at Danmark er dybere involveret end hidtil kendt i NSA's globale spionage. Talepapiret er blandt en række klassificerede NSA-dokumenter, som Information i dag lægger frem

Snowden-dokumenter afslører dansk partnerskab med NSA

FE indgår i et partnerskab med NSA om at tappe danske fiberkabler med tele- og internettrafik, fremgår det af tophemmelige NSA-dokumenter. Tilsyneladende er Danmark del af et hidtil ukendt overvågningsprogram, der kan føre til, at også danskere bliver mål for den amerikanske efterretningstjeneste

Af Sebastian Gjerding, Henrik Moltke, Anton Geist og Laura Poitras

Forsvarets Efterretningstjeneste (FE) deltager efter alt at dømme i et hidtil hemmeligholdt samarbejde med National Security Agency (NSA) om at tappe fiberkabler, der transporterer internet- og teletrafik gennem Danmark. Dermed ser Danmark ud til at være blandt de lande, der medvirker til at opfylde NSA's målsætning om at kunne opfange enhver elektronisk kommunikation hvor som helst i verden.

Det dansk-amerikanske samarbejde om at tappe kabler er omtalt i et talepapir udarbejdet til den daværende direktør for NSA, den firestjernede general Keith Alexander, i forbindelse med et møde mellem medarbejdere fra NSA og deres danske kolleger fra FE i sommeren 2012.

»Understreg NSA's engagement i den særlige adgang og i at assistere FE med at håndtere adgangen. Påmind danskerne om det langvarige NSA-FE-partnerskab om at arbejde med kabeladgang med.«, står der i talepapiret.

Sidste sætning er således ufuldstændig, og ligesom der kan være tale om en simpel fejl, kan det ikke udelukkes, at noget aktivt er blevet udeladt, eksempelvis oplysninger om en tredje aktør udover NSA og FE. Tilbage står dog, at NSA og FE tilsyneladende har et samarbejde om kabeladgang.

Talepapiret er stemplet 'tophemmeligt', det højeste klassifikationsniveau i USA. Information har fået adgang til det og en række andre klassificerede NSA-dokumenter via whistlebloweren Edward Snowden.

Oplysningerne i Keith Alexanders talepapir om en dansk-amerikansk kabeladgang stemmer overens med oplysninger i et andet tophemmeligt dokument vedrørende NSA's forhold til FE. I dokumentet skriver NSA, at tjenesten forsyner sin danske søsterorgani-

→ Fortsættes side 2

FOKUS Partnerskab med NSA

Snowden ...

Fortsat fra forsiden

sation med »indsamlings- og behandlingsudstyr«, og som det fremgår af dagens Information, er netop denne form for assistance fra NSA's side fast procedure i forbindelse med partnerskaber om kabel-adgang med såkaldte tredjepartslande som Danmark.

Villig til at løbe risici for USA

Adgangen til fiberkabler er en hjørnesten i NSA's globale masseovervågning og er med til at muliggøre den efterretningsmæssige »guldalder«, som NSA omtaler nutiden i en strategierklæring. »Internettets rygrad« kaldes kablerne, der transporterer telefonopkald og internettrafik, det vil blandt andet sige e-mails, Skype-opkald og Facebook-beskeder.

Tilsyneladende er samarbejdet mellem NSA og FE en del af et omfattende, internationalt NSA-program om kabeladgang med kodenavnet RAMPART-A, som Information i dag kan afsløre. Programmet går ud på, at NSA samarbejder med en række af de i alt 33 såkaldte tredjepartslande, som Danmark er iblandt, om kabeladgange på partnerlandenes territorium.

At Danmark dermed ser ud til at være blandt de tredjepartslande, der spiller en central rolle i forhold til at muliggøre NSA's overvågning af verdensomspændende elektronisk kommunikation, stemmer overens med, at NSA i flere dokumenter beskriver FE som en særlig vigtig samarbejdspartner.

I dokumentet om relationen mellem FE og NSA omtales den danske efterretningstjeneste eksempelvis som »en af NSA's betroede og pålidelige SIGINT (elektronisk indhentning af kommunikation, *red.*) -partnere« og som »en af NSA's bedste antiterrorpartnere«, der ofte som de første »tilbyder assistance« og »er villig til at løbe risici på vegne af USA«.

Den russiske forbindelse

Et lands værdi som partner for NSA's samarbejder om kabeladgang afgøres af, hvilken trafik der strømmer igennem fiberkablerne på landets territorium.

»Hvis dit land er et vigtigt sted i netværket, er du en vigtig partner for NSA,« siger Mikko Hyppönen, der er forskningschef i finske F-Secure og en af verdens førende eksperter inden for datasikkerhed. »Danmark er et af de lande. Megen international trafik fra Skandinavien og Rusland går gennem danske netværk, og det begrunder interessen for at samarbejde med danske myndigheder,« vurderer Hyppönen.

Han tilføjer, at også store mængder trafik fra Tyskland passerer Danmark: »Det er ikke noget, den almindelige netbruger tænker over, men mange tyskere forbinder f.eks. til Facebook og Google-tjenester via Danmark, fordi både Google og Facebook har store datacentre i Norden, og den trafik går overvejende gennem Danmark.«

Forskningschef i det internationale teletrafikanalysefirma TeleGeography, Alan Mauldin, fremhæver også Danmarks russiske forbindelse som en mulig grund til NSA's interesse i en dansk kabeladgang.

»Der er fire hovedruter, som forbinder Rusland med Europa. En af dem er via Skandinavien. Hvis man er interesseret i at aflytte international russisk kommunikation, så kunne Danmarks fysiske placering som et transitpunkt, der kæder Rusland sammen med andre lande, være en årsag.«

En gensidig aftale

I de fiberkabler, der krydser Danmark, passerer både international og dansk trafik. NSA har dermed adgang til kabler med dansk data, selv om det står klart, at den amerikanske tjeneste ikke holder sig tilbage fra at spionere imod sine allierede blandt tredjepartslandene. Om forholdet til tredjepartslandene står der således i et NSA-dokument, som det tyske nyhedsmagasin Der Spiegel tidligere har fremlagt: »Vi kan indfange elektroniske signaler fra de fleste udenlandske tredjeparts-partnere og gør det ofte.«

NSA's dokumenter om RAMPART-A-programmet tyder dog på, at visse retningslinjer skal forhindre den amerikanske efterretningstjeneste i at udnytte adgangen i et partnerland til at spionere direkte imod landets borgere. Det fremgår således, at det enkelte partnerland kan følge med i, hvilke overordnede kategorier, NSA indhenter data ud fra i forbindelse med en kabeladgang. Det nævnes også i et dokument, at der findes lister over emner og mål, som NSA af hensyn til partnerlandene ikke søger efter i den enorme datamængder, som tjenesten får adgang til ved en kabeladgang. Desuden står der i en RAMPART-A-præsentation: »Partner indsamler ikke mod USA, USA indsamler ikke mod værtslandet.«

Samme bemærkning gentages i en overordnet præsentation af NSA's fiberprogrammer, men her tilføjes en mindre, men bemærkelsesværdig modifikation fra NSA's side: »der ER undtagelser«.

Bemærkelsesværdigt er det, at reglen om ikke at spionere imod partnerlande fremgår af et dokument, der er klassificeret på en sådan måde, at oplysningerne deri må deles med de allierede efterretnings-

FAKTA

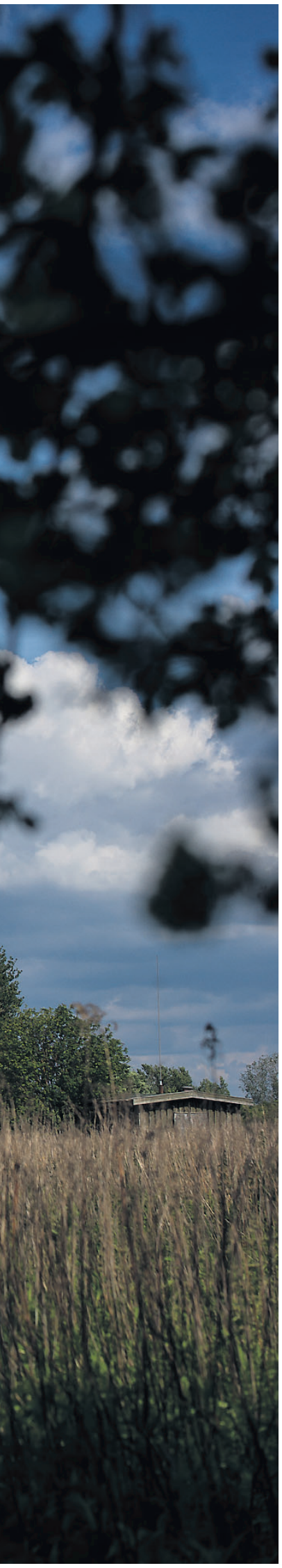
NSA's allierede

Andenparter:

- NSA's såkaldte andenparter indgår i den såkaldte FIVE EYES-alliance og udgøres udover USA af de angelsaksiske lande Storbritannien, Canada, Australien og New Zealand. Det er de lande, som NSA arbejder tættest sammen med, og som særligt assisterer amerikanerne i deres globale spionageoperationer. Samarbejdet om tapning af fiberkabler, som involverer andenparter, har kodenavnet Windstop og involverer først og fremmest Storbritannien.

Tredjeparter:

- Danmark har en såkaldt tredjepartsrelation til NSA. Tredjepartslandenes efterretningstjenester har et samarbejde med NSA, men et mindre tæt samarbejde end tjenesterne i andenpartslandene. Ifølge en opgørelse fra 2013 har 33 lande et tredjeparts-forhold til NSA, men med store variationer i den konkrete relation. Samarbejdet med tredjeparter varierer og kan både indeholde støtte til mindre konkrete operationer og til årelange samarbejder om masseovervågning. Samarbejdet mellem NSA og tjenestens tredjeparter om tapning af fiberkabler har kodenavnet RAMPART-A.



Ifølge dokumenter om RAMPART-A-programmet arbejder mange af NSA's partnerlande med data fra fiberkabler under dække af satellit-operationer, som alligevel er tydelige i landskabet. I Danmark har FE blandt andet satellit-operationer på Amagers sydspids, Aflandshage.
Foto: Jakob Dall

tjenester i andenpartslandene, mens undtagelsen fra reglen fremgår af et dokument, der specifikt ikke må deles med statsborgere i noget andet land end USA.

Hvilke undtagelser, der findes fra reglen om ikke at udnytte en kabeladgang til at spionere imod et partnerland, fremgår ikke, ligesom det står ubesvaret hen, hvilke muligheder for repressalier en partner har, hvis NSA forbryder sig mod aftalen.

Filtrering af data

Tidligere har FE-chef Thomas Ahrenkiel sagt til Politiken, at den danske efterretningstjeneste deler data indsamlet »i et konfliktområde i udlandet« med NSA. I den forbindelse udtalte Thomas Ahrenkiel: »Skulle der være danskrelaterede data, så har vi nogle filtre, der renser dem for danske informationer, inden de udleveres til partnere.«

Ifølge en kilde med kendskab til FE's filtrering af data fra en konfliktzone vil noget lignende være tilfældet med data indsamlet ved kabeltap i Danmark. Der er dog tale om en relativ grov filtrering, der eksempelvis frasorterer. dk-mailadresser, men som ikke opfanger eksempelvis danskere med gmail.com-adresser. Det skyldes formodentlig, at præcis filtrering af såkaldte rådata reelt er umulig, og som det fremgår af dagens avis, er FE tilsyneladende heller ikke juridisk forpligtet til at rense rådata for danskeres data før overlevering til en tjeneste som NSA.

Thomas Ahrenkiel har ikke ønsket at hverken be- eller afkræfte eksistensen af et dansk-amerikansk samarbejde om kabeladgang over for Information, og han har derfor heller ikke ønsket at udtale sig om, hvorvidt der i givet fald anvendes filtre på rådata indsamlet fra kabler i Danmark.

Intet magisk ved dansk data

Under alle omstændigheder vil Danmark dog næppe få meget ud af at forsøge at sikre sig mod udlevering af danskeres data fra en dansk-amerikansk kabeladgang. Det vurderer den amerikanske it-sikkerhedsekspert Bruce Schneier, der har et indgående kendskab til NSA.

Han peger på, at NSA vil kunne tappe danskeres data gennem andre adgange i andre lande, hvor dansk data passerer igennem. Ved at indgå aftaler med en række lande om at modtage data fra fælles kabeladgange med den ene begrænsning, at NSA ikke må indsamle data fra de pågældende landes borgere, kan NSA således opbygge et system, der sikrer, at data fra alle lande kan indsamles, vurderer Schneier, der har set en del af Informations dokumenter om RAMPART-A.

»Der er intet magisk ved dansk data, som gør det immunt over for at blive opsnappet andre steder,« siger han.

Bruce Schneier tilføjer: »NSA forsøger at indsamle alt, og ved at give dem adgang til internet-knudepunkter i Danmark er I med til at sætte dem i stand til det. Det er her, NSA spiller jer alle sammen ud mod hinanden. I får sikkert adgang til den del, I selv forsyner NSA med. Men den del er kun af begrænset værdi. Den egentlige værdi er det hele samlet, og det får NSA. På den måde giver I dem mere, end I får retur. Det er faktisk en dårlig handel for jer.«

Også Edward Snowden advarede tidligere i år om ulemperne for part-

→ Fortsættes på side 4

> **NSA forsøger at indsamle alt, og ved at give dem adgang til internet-knudepunkter i Danmark er I med til at sætte dem i stand til det**
>
> **Bruce Schneier**
> amerikansk it-sikkerhedsekspert

DOKUMENTATION

Dokumentet, hvor et samarbejde mellem NSA og FE om kabelindhentning bliver nævnt, er fra marts 2013. Det indeholder NSA-direktør Keith Alexanders talepunkter til et planlægningsmøde med medarbejdere fra FE i juni 2012. DENUSA er titlen på mødet, der andetsteds i NSA-dokumenterne beskrives som »den årlige strategiske NSA-FE planlægningskonference«.

Klassifikationsoplysningerne ud for det centrale afsnit om kabeladgang viser, at oplysningerne er tophemmelige (TS), som er det højeste generelle klassifikationsniveau i USA, og at der er tale om 'special intelligence' (SI), hvilket er betegnelsen for oplysninger, der har med monitorering af elektronisk kommunikation at gøre. Oplysningerne må kun udleveres til USA og Danmark (REL TO USA, DNK).

SECRET//REL TO USA, AUS, CAN, GBR, NZL

DENUSA

6-8 June

(S//REL TO USA, DNK) Thank the Danes for their wonderful hospitality they extended to you and your delegation during your March visit to Copenhagen.

(TS//SI//REL TO USA, DNK) [redacted]

(S//REL TO USA, DNK) [redacted]

(TS//SI//REL TO USA, DNK) Emphasize NSA's commitment to the special access and assisting DDIS in managing the access.

Remind the Danes of the long NSA-DDIS partnership working cable access with.

Note that we look forward to new areas of cooperation.

I dokumentets centrale passage omtaler Keith Alexander samarbejdet mellem NSA og FE om en kabeladgang. Det fremgår, at der er tale om et »partnerskab«, og at NSA »assisterer« FE med at håndtere adgangen. Tilsyneladende omtaler NSA også kabeladgangen som en »særlig adgang«, hvilket er en betegnelse, der går igen i dokumenter om RAMPART-A-programmet.

'Working cable access with.'

Det er uklart, hvorfor sætningen er ufuldendt. Det kan være en fejl. Eksempelvis kan der have skullet stå » ... working with cable access«, og ordet 'with' er så blevet placeret på den forkerte side af 'cable access'.
En anden forklaring kunne være, at et eller flere ord, der beskriver endnu en aktør, som er involveret i kabelindhentningen, er udeladt.

SAMFUND

Politiet bruger allerede kropskameraer – mod borgerne

Task Force Pusher Street benytter kropskameraer 'i stor stil' på Christiania, fordi de virker afskrækkende og kan bruges som bevismateriale i retten. Oplysningerne får ikke Politiforbundet til at ændre holdning til sagen, mens advokat Knud Foldschack er betænkelig ved kropskameraerne, fordi politiet tidligere er blevet taget i at manipulere med fotobeviser

Af Sebastian Stryhn Kjeldtoft

Debatten om kropskameraer på politibetjente er blusset op, efter Enhedslistens i sidste uge foreslog en forsøgsordning i to politidistrikter. Blandt andet har Politiforbundets formand Claus Oxfeldt udtalt sig kritisk om udspillet, som han mener krænker borgernes retsstilling og er et udtryk for »mistillid til politiet«.

Men nu viser det sig, at dansk politi allerede bruger kropskameraer – og har gjort det længe.

Når politibetjentene fra Task Force Pusher Street er på 'gåtur' på Christiania, er de små kropskameraer monteret på vesten. Det forklarer politikommissær Steffen Thaaning Steffensen fra Københavns Politis Task Force Pusher Street.

»Vi har gode erfaringer med kropskameraer. De hjælper os med at fange nogle af de banditter, vi ellers ikke ville få fat i. Så sent som i forrige uge anholdte vi tre personer, der kastede med sten efter politiet, og som vi kunne identificere ud fra optagelserne. Vores øjne kan opfange noget, men kameraerne opfanger ofte noget andet, og derfor bruger vi dem i stor stil,« forklarer Steffen Thaaning Steffensen.

Ifølge politikommissæren hjælper kropskameraerne med at gøre »beviserne stærkere« i en efterfølgende retssag. Derudover mener han, det afskrækker nogle borgere på Pusher Street fra at begå kriminelle handlinger, fordi de ved, de bliver filmet.

I Enhedslistens forslag, som støttes af Dansk Folkeparti, SF, Konservative og Liberal Alliance, skal videomaterialet fra kropskameraerne kunne indgå som bevismateriale i klagesager mod politiet. En såkaldt tovejs-overvågning. Men Task Force Pusher Streets optagelser kan kun bruges til at tiltale borgerne.

– Jeres kropskameraer bruges mod borgerne. Men i den aktuelle debat vil fem partier i Folketinget åbne op for, at den slags videomateriale også kan bruges af borgerne i sager mod politiet. Hvad tænker du om det?

»Det har jeg ingen holdning til. Jeg tager mig af det operative politiarbejde. Hvad angår det politiske må du spørge mine chefer længere oppe i systemet,« lyder det fra politikommissær Steffensen.

Oxfeldt: 'Ikke det samme'

Politiforbundets formand Claus Oxfeldt har tidligere kritiseret Enhedslistens forslag i skarpe vendinger i Information:

»Faktum er, at kropskameraer i Danmark er at skyde gråspurve med kanoner, og det vil være forfærdeligt for borgernes retsstilling,« forklarede Oxfeldt til Information sidste onsdag. De nye oplysninger om, at politiet allerede benytter kropskameraer regelmæssigt, får imidlertid ikke Oxfeldt til at ændre holdning:

»Jeg var, før den her debat startede, ærlig talt ikke vidende om at politiet allerede bruger kropskame-

> **Vi har gode erfaringer med kropskameraer. De hjælper os med at fange nogle af de banditter, vi ellers ikke vil få fat i**
>
> **Steffen Thaaning Steffensen**
> Københavns Politis Task Force Pusher Street

Politiets Task Force for Christiania har haft stor glæde af at bruge kropskamera på betjentene i aktioner på fristaden. Kropskameraer har i flere tilfælde hjulpet politiet med at identificere og fange kriminelle.
Foto: Bax Lindhardt/Scanpix

raer i så vid udstrækning, som det er tilfældet. Men det her er noget andet, for politiet bruger det som efterforskningsmiddel. Enhedslistens forslag skal pålægge politiet at bruge kameraer, som kan bruges i klagesager,« siger Claus Oxfeldt.

– Er forskellen ikke bare, at i det forslag Enhedslisten har stillet, der kan optagelserne også bruges mod politiet, hvor optagelserne i dag kun kan bruges mod borgerne?

»Nej, det synes jeg er en forkert måde at sige det på. Der er forskel på pligten til at bære et kamera hele tiden, og så at bruge et kamera til en efterforskning. Det er jo ikke anderledes, end når vi laver rum- eller telefonaflytning. Det er et middel.«

– Hvorfor må optagelserne så ikke bruges til klagesager mod politiet?

»Jamen som jeg sagde sidst: Hvis ikke man har tillid til politiet, så luk det da. Den tillid må vi simpelthen have i et retssamfund, at det politimanden siger, det er rigtigt. Man er simpelthen nød til at våge det ene øje og tro på, at vi ikke stjæler fra de kriminelle, at vi ikke overfalder borgerne – at vi har ordentlige, fornuftige politibetjente,« forklarer Oxfeldt.

»Mange af klagerne mod politiet i dag er jo helt banale. Jeg har et eksempel på en klage, hvor politibetjenten sagde 'hav en fortsat god dag' – det opfattede borgeren som arrogant. Langt de fleste klager er af den type.«

Han er dog åben over for kropskameraer på betjente, hvis videomaterialet alene kan bruges som bevismateriale i klagesager mod politiet – modsat i dag, hvor videomaterialet alene kan bruges mod borgerne:

»For så kan kropskameraet bruges til at klarlægge, hvad den pågældende betjent har set – eller burde have set, eller i forbindelse med klager om voldelig adfærd. I så fald er det et fremragende forslag. For efter COP15 var der vist en bakterie i omløb i politiets regi, da de skulle genhuske, hvad de så og oplevede under demonstrationerne. For betjentenes vidneudsagn var jo direkte i strid med virkeligheden,« siger Foldschack.

Den anklage bliver mødt med hovedrysten fra Claus Oxfeldt:

»Jeg synes, udtalelsen taler for sig selv. Det er sørgeligt, en advokat kan sige sådan noget,« lyder det kortfattet.

Foldschack mener dog, han har retten på sin side:

»Desværre er det jo bevist, at vi har haft tusindvis af sager om administrativ frihedsberøvelse. De er altså ikke gratis for samfundet. Og vi har vundet dem alle sammen. Oxfeldt er bare en, der altid siger nej til noget, der kan højne retssikkerheden og afhjælpe den her problemstilling.«

sebk@information.dk

Foldschack er bekymret

Den udlægning af politiets virke er advokat Knud Foldschack uenig i. Han har ført sager for christianitterne på Christiania og frihedsberøvelserne under COP15, hvor 2.000 borgere efterfølgende modtog erstatning fra staten. Foldschack er »meget bange« for politiets brug af kropskameraer, fordi han mener, politiet før har manipuleret med den slags bevismateriale i retssagerne efter COP15:

»Vi fik fremlagt billeder af knive og gasmasker, som politiet sagde var blevet fundet på gader, biler og i andre lokaler. Det så ud som om, de havde fundet bevismateriale på fire lokationer – men vi fandt ud af, at det var de samme genstande, som bare var blevet flyttet og affotograferet flere steder,« forklarer Foldschack, som også oplevede, at fotos blev lysmanipuleret, så en farvet jakke pludselig fremstod som mørkt tøj.


SAMFUND
Noter
Præcisering
Thorning: Stadig tale om asyl-stramning
Pernille Skipper får plads i Kontroludvalg
Politiforbundet: 'Så luk da bare hele politikorpset!'

Enhedslisten foreslog i sidste uge en forsøgsordning med kropskamera på betjente. Det fik politiforbundets formand Claus Oxfeldt til at udtale sig kritisk om udspillet, som han mener krænker borgernes retsstilling og er et udtryk for 'mistillid til politiet'.

Noter

Embedsmænd står til kritik i skattesag

■ Embedsmænd står til at modtage forholdsvis hård kritik, når Skattesagskommissionen offentliggør sin endelige beretning om statsminister Helle Thorning-Schmidt (S) og hendes mand, Stephen Kinnocks skattesag. Men der er ikke lagt op til, at nogen skal drages til ansvar for magtfordrejning ved at forsøge at påvirke afgørelsen i skattesagen, skriver Berlingske søndag.

Berlingske har haft adgang til flere af sagens dokumenter. De peger blandt andet på, at Peter Loft, daværende departementschef i Skatteministeriet, gik for tæt på Thornings sag. Men kommissionen vurderer, at Loft har handlet uagtsomt. Flere af skattesagens hovedpersoner vurderes at kunne have overtrådt deres tavshedspligt ved at videregive et rygte om, at Stephen Kinnock er homoseksuel.

Samtidig frikender beretningen, ifølge Berlingske, i grove træk Troels Lund Poulsen, men tror ikke på hans vidneforklaringer om, hvor lidt han interesserede sig for sagen. Tidligere spindoktor Peter Arnfeldt, der fortsat er sigtet for at lække Thornings skattepapirer til pressen, står til at blive frikendt. Ifølge kommissionen er der ikke grund til at tro, at han forsøgte at lække papirerne. Ritzau

Politisk mistillid til Justitsministeriet

■ Justitsministeriet tilbageholder oplysninger, udsender forkerte asyltal og modarbejder Folketingets Retsudvalg, siger flere retsordførere ifølge Jyllands-Posten. Især nager den såkaldte Christiania-sag stadig. Den kostede sidste år Morten Bødskov (S) posten som justitsminister, mens de involverede topembedsmænd blev frikendt for ansvar i sagen om det omstridte aflyste besøg på Christiania. Det skete med henvisning til det nye juridiske begreb 'nødløgn'.

»Den løgn ligger som en tyk tåge hen over hele forholdet mellem Justitsministeriet og retsudvalget. Og i det hele taget forvrides, fordrejes og ruttes der ikke med sandheden i Justitsministeriet, siger DF's retsordfører, Peter Skaarup. Venstres retsordfører, Karsten Lauritzen, mener, at kernen af problemet er en manglende respekt for de folkevalgte politikere, og han har ikke længere den store tillid til ministeriet: »Der er et farligt kulturproblem i ministeriet,« siger han.

Flere ordførere, heriblandt SF's retsordfører, Karina Lorentzen, oplever, at de generelt har svært ved at få svar på folketingsspørgsmål fra ministeriet. Ritzau

Corydon til KL: Der er penge til flygtninge

■ Med KL-formand Martin Damm (V) i spidsen kræver kommunerne fuldt fokus på flygtninge i forhandlingerne om næste års finanslov.

Til det siger finansminister Bjarne Corydon (S). »Regeringen har fundet de penge, der skal til for at løfte opgaven.«

Regeringen har bl.a. taget 2,5 milliarder kr. fra ulandsbistanden til at finansiere de forventede 20.000 asylansøgere næste år. I alt forventes der merudgifter på 4,5 milliarder kroner. Ritzau

Kryptering

»Personlig kryptering er lidt ligesom genbrug. Du får det godt, men det gør ikke den store forskel«

Aktivister og rettighedsorganisationer har siden Snowden-afsløringernes begyndelse råbt på tekniske ændringer, der kan sikre privatlivet. IT-giganter som Apple og Google er begyndt at lytte, og krypteringsteknologi dukker op i alt fra iPhones til netbrowsere. Men politi og efterretningstjenester går nu til modangreb mod det, de kalder en direkte hjælp til pædofile og terrorister. Krypteringskrigen er brudt ud igen

AF SEBASTIAN GJERDING

Den amerikanske hacker Jacob Appelbaum står foran et par hundrede mennesker i Bremen Teater i København. De er mødt op for at lære mere om krypteringsteknologi, og om hvordan de beskytter deres e-mails, chats og internetbrug. Og for at høre Appelbaum fortælle om, hvorfor det er så nødvendigt at gøre:

»Der udkæmpes et stort slag lige nu. Stater over hele verden prøver at forhindre almindelige mennesker i at få adgang til kryptering og i at forstå, hvordan det virker,« siger han.

Arrangementet i Bremen Teater er et såkaldt Cryptoparty og afholdes i forbindelse med premieren på *Citizenfour,* dokumentarfilmen om Edward Snowden. Det er det største arrangement af den karakter i Danmark til dato – og udtryk for en global krypteringskrig, der på ny er brudt ud efter Snowden-afsløringerne. Krigen har mange aktører, men den handler dybest set om, i hvor høj grad teknologi skal bidrage til at sikre menneskers kommunikation og privatliv mod udenforstående – herunder også mod statslige efterretningstjenester og politi. Kravet om teknikken som garanten for beskyttelse af privatlivet er blevet mere højlydt det seneste år, og en del teknologivirksomheder er begyndt at lytte.

I sidste måned varslede Apple og Google nye krypteringsinitiativer, mens den populære beskedtjeneste WhatsApp i denne uge offentliggjorde, hvad de selv kalder »den største implementering af end-to-end krypteret kommunikation i historien« til sine millioner af brugere.

Jacob Appelbaum er en af drivkræfterne bag Tor-projektet, der gør det muligt at surfe anonymt på internettet, og har også selv været bidragyder til nogle af de mest opsigtsvækkende afsløringer baseret på Snowden-dokumenter. Historierne har været med til at sætte global dagsorden i halvandet år, og de har givet offentligheden et historisk stort indblik i staternes gigantiske, digitale overvågningsapparater.

Til gengæld har de stort set ikke haft nogen politiske konsekvenser. I hverken Danmark, Storbritannien eller USA er der flertal for at begrænse efterretningstjenesternes råderum, og selv en mindre reform af en specifik indsamling rettet mod amerikanske borgeres telefondata faldt i denne uge til jorden i det amerikanske senat.

Ifølge Jacob Appelbaum er politiske reformer heller ikke nok. Menneskerettigheder, konventioner og krav om dommerkendelser på nationalt plan forhindrede ikke opbygningen af overvågningsapparatet, for politik og jura kan ikke sikre folks data mod efterretningstjenesterne uden hjælp fra teknikken. Flere af Snowden-afsløringerne har handlet om, hvordan efterretningstjenesterne er gået videre end deres i forvejen vide adgang til data gennem henvendelser til det enkelte data-firma ved hjælp af retskendelser. Det juridiske krav om retskendelser var i praksis ikke nogen beskyttelse, fordi det var nemt for tjenesterne at gå videre end det. Hverken juraen eller politikken formåede at beskytte individets rettigheder, og derfor er det nu op til en udbredelse af krypteringsteknologien at sikre dem:

De embedsmænd, der bruger så meget tid på at kritisere Apple, burde lægge den følelse af total berettigelse, som de har udviklet de seneste syv år, fra sig og bruge noget tid på at takke Apple og Google for at have gjort det så nemt for dem så længe

— KEVIN POULSEN

»Vi kan ikke stoppe infiltrationen, men vi kan påvirke dens skala. Ved at bruge stærk kryptering kan vi ændre på deres stordriftsfordele og dermed ændre den måde, hvorpå data bliver værdifulde for andre mennesker og specifikt for spionerne. Jo mere de bliver nødt til at arbejde for den, desto mere vil de kun gøre det med de mennesker, som rent faktisk er virkeligt værdifulde for dem,« siger Jacob Appelbaum.

Problemet er altså ifølge Appelbaum, at den sikkerhedssvage teknologi har gjort det for billigt for efterretningstjenesterne at overvåge, og for at ændre på den situation kræver det mere end bare, at de få hundrede mennesker i Bremen Teater lærer at bruge kryptering.

»Personlig kryptering er lidt ligesom genbrug og global opvarmning. Du får det bedre med dig selv, men det gør ikke den store forskel,« siger Jacob Appelbaum.

De pædofiles telefon

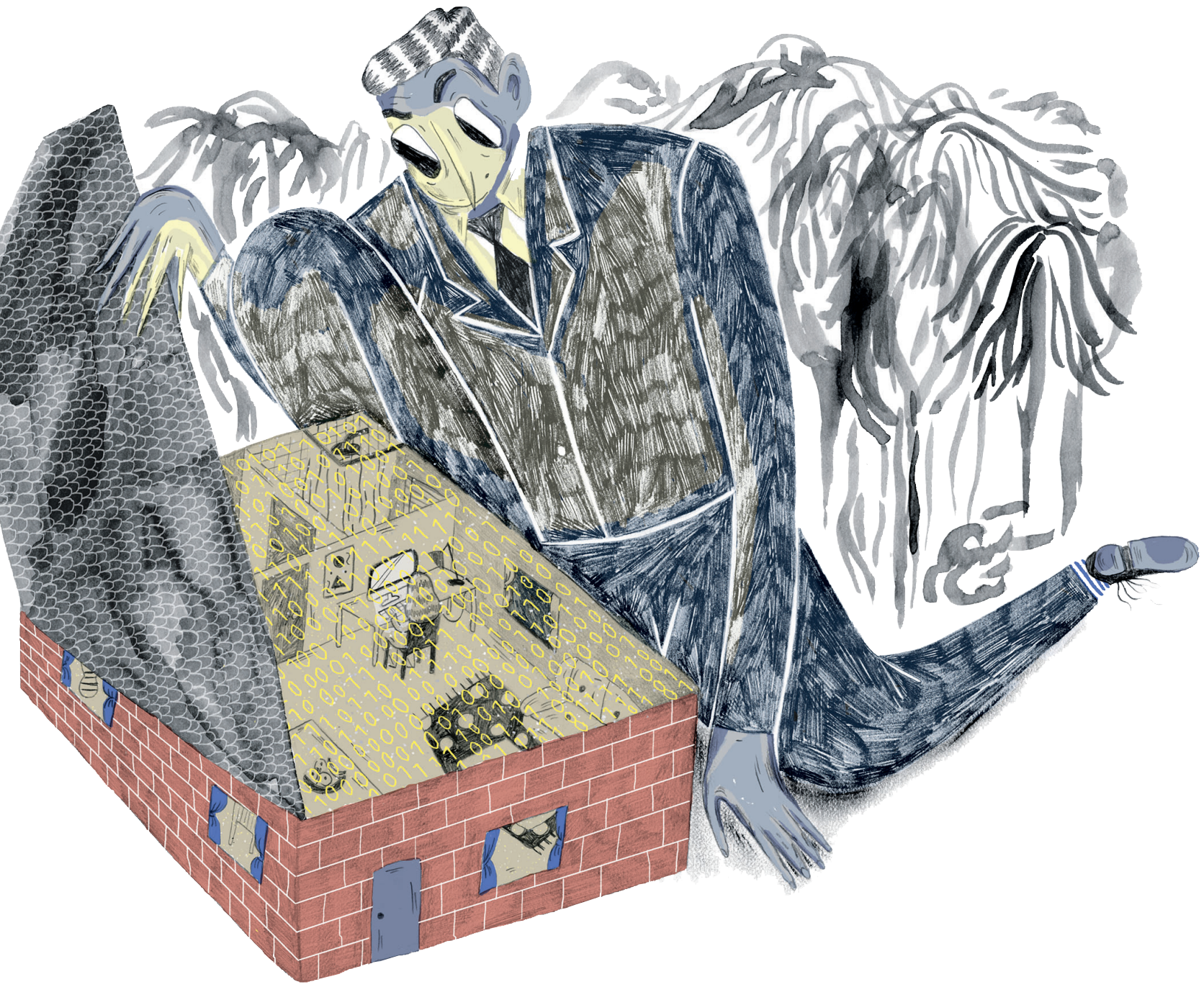
»Det gør en forskel rent individuelt, og du bør selvfølgelig gøre det, men for at skabe en gennemgribende social forandring, så kræver det at der sker noget på industrielt niveau. Vi må ikke bare kræve, at verdens regeringer ændrer politik, men også kræve den teknologi, som politikken nødvendiggør.«

At de store selskaber er begyndt at blive mere opmærksomme på privatlivshensyn og sikkerhed kommer, efter at Snowden-dokumenterne har afsløret, at flere af dem har et meget nært forhold til efterretningstjenesterne. Andre af de lækkede dokumenter viste dog også, hvordan efterretningstjenesterne udnytter dårligt designede systemer hos selskaberne uden deres medvidende. Washington Post tog den britiske efterretningstjeneste GCHQ i at omgå Googles sikkerhedssystemer ved at tappe fiberkablerne direkte, når Google løbende flyttede sine brugeres data ukrypteret imellem sine datacentre over hele verden. GCHQ's genialt udtænkte plan gjorde reelt tjenesten i stand til at få adgang til milliarder af emails uden retskendelse eller henvendelse til Google og blev illustreret på en af efterretningstjenstens egne slides med en glad smiley. En smiley, der nu ser ud til at give bagslag:

»Efter at Google blev angrebet af den britiske version af NSA, blev vi irriterede. Så vi satte *end to end*-kryptering på vores systemer, så det praktisk talt bliver umuligt for en hvilken som helst indtrænger at få adgang,« sagde Google-chef Eric Schmidt til en paneldebat i sidste måned.

Det er nye toner fra et af de selskaber, der ellers ikke er kendt for at være fjendtligt indtillede overfor myndighederne, og meget tyder på, at kryptering er blevet et konkurrenceparameter. Apple offentliggjorde i september, at deres nye iPhone 6 leveres med stærk kryptering af de data, der ligger på telefonen, og Google har lignende planer om at gøre stærk kryptering til standarden i styresystemet Android.

Selv om der stadig er tale om relativt begrænsede initiativer, har udviklingen medført en hård reaktion fra myndigheder og efterretningstjenester. FBI's direktør James B. Comey har anklaget selskaberne for at give de kriminelle forbedrede muligheder. Sel-



Teknik. ***Det seneste års afsløringer af masseovervågningen viser, at lovgivning ikke hjælper, hvis det teknisk er for nemt for efterretningstjenesterne at omgå den. Derfor er der brug for en teknologi, som gør den massive overvågning af alt og alle umulig.*** *Tegning: Jesephine Kyhn/iBureauet*

skabernes intiativer er ifølge FBI-chefen et eksempel på, at 'post-Snowden pendulet' er svinget for langt til den ene side:

»Det, der bekymrer mig med disse selskaber, er, at de markedsfører noget, som eksplicit gør det muligt for folk at være hævet over loven,« siger han til New York Times.

»Forestillingen om, at nogen ville markedsføre et skab, som aldrig kan åbnes – selv hvis det involverer en børnekidnapper og en retskendelse – giver for mig ingen mening.« Chefen for Chicagos politi, John J. Escalante, var ude med endnu hårdere udtalelser og spåede, at »Apple vil blive den pædofiles foretrukne telefon«, mens den nye direktør for den britiske efterretningstjeneste GCHQ, Robert Hannigan, fokuserede på kommunikationselskabernes rolle i kriminaliteten:

»Jeg forstår godt, hvorfor de har et anstrengt forhold til regeringer. De stræber efter at være neutrale transportører af data og at sidde uden for eller over politik. Men i stigende grad bliver deres tjenester ikke kun brugt til at *hoste* materiale, der er voldeligt, ekstremistisk eller børneudnyttende, men er også selve den rute, der faciliterer kriminalitet eller terrorisme,« skrev han i et debatinlæg i forbindelse med sin tiltrædelse.

»Hvor lidt de end kan lide det, så er de blevet kommando-og-kontrol netværket for terrorister og kriminelle, som finder deres tjenester lige så transformerende, som alle os andre.«

Myndighederne overreagerer

Den hårde reaktion fra myndighederne på særligt Apple og Googles initiativer er bemærkelsesværdig, fordi det er så relativt begrænset, hvad de to firmaer reelt kommer til at kryptere. Der er tale om et initiativ, der som standard beskytter den data, der ligger på telefonen med en adgangskode, som kun brugeren har og altså hverken firmaet eller myndigheden kan få låst op. Myndighederne vil dog stadig kunne få adgang til data om, hvem der kommunikeres med, de kan aflytte kommunikationen centralt, bevægelsesmønstre kan kortlægges, mens også alle dem, der bruger iCloud til backup vil stå uden for den nye beskyttelse. Men det er stadig en beskyttelse, der kan afskære myndighederne fra adgang til information, og som ifølge FBI-chef James B. Comey »truer med at føre os alle sammen til et meget mørkt sted«:

»Kryptering er ikke noget nyt. Men udfordringen for myndighederne og ansvarlige for den nationale sikkerhed er markant større efter de nylige standardkrypteringsindstillinger og krypterede enheder og netværk – alt sammen designet til at øge sikkerheden og privatlivet,« sagde Comey i en tale i oktober.

Ifølge Ivan Damgård, der er professor ved Institut for Datalogi på Aarhus Universitet med speciale i kryptering, ser myndighederne ud til at overreagere. Men reaktionen er et tegn på, at de ikke helt ved, hvordan de skal håndtere selskabernes nye modstand:

»Hvis man skal se på dem, man reelt kan frygte får adgang til stærk kryptering – som organiserede kriminelle og terrorgrupper – så er det jo alt, alt for sent at forhindre deres adgang. Det er jo kendt åben forskning, hvordan man krypterer, så dem, man for alvor frygter, kan jo allerede gøre det og har kunnet det længe,« siger han.

»Spørgsmålet er, hvad man overhovedet kan gøre? Katten er ude af sækken for længe siden. Det bliver man nødt til at erkende,« siger Ivan Damgård.

Fordør eller bagdør?

Slagsmålet i USA minder i høj grad om den diskussion, der fandt sted i 1990'erne, da man fra især amerikanske myndigheders side forsøgte at undgå at stærk kryptering overhovedet kom på markedet, uden at de var sikret en særlig privilegeret adgang. Diskussionen blev kaldt krypteringskrigen, og NSA og efterretningstjenesterne endte med at tabe slaget. Men konsekvensen af deres nederlag var ifølge Ivan Damgård ikke særligt hensigtsmæssigt, for da NSA ikke fik lovlig adgang til alle data begyndte de i stedet at sikre sig adgang alligevel ved at svække internettets sikkerhed og angreb kernepunkter i alverdens netværk: »Da NSA ikke kunne få adgang gennem fordøren, så tog de bagdøren,« som Ivan Damgård formulerer det.

»Det gør en forskel rent individuelt, og du bør selvfølgelig gøre det, men for at skabe en gennemgribende social forandring, så kræver det, at der sker noget på industrielt niveau«

— JACOB APPELBAUM

»Nu har man så fået presset Apple og Google op i et hjørne, så de føler, at de ikke kan være sikre på deres forretning uden for USA, med mindre de sørger for at lægge ansvaret fra sig ved ikke selv at kunne genskabe brugernes data,« siger han.

»Men måske skulle man overveje, hvordan man alligevel kan sikre en legal adgang for myndighederne under visse betingelser. Selv om det er imod manges principper,« siger Ivan Damgård. En sådan mulighed for at få adgang ad »fordøren« taler efterretningstjenesterne også selv om, men de fleste kritikkere hævder, at der reelt ikke er tale om en forskel på en bagdør og en fordør. Den slags systemer vil altid kunne misbruges og udnyttes af både efterretningstjenester, hackere og cyberkriminelle. I stedet bør politiet og myndighederne lære at leve med, at der findes begrænsninger, skriver den tidligere hacker og redaktør på Wired Kevin Poulsen.

»Smartphones har været en guldmine for politiet, og den lille korrektion som stærk kryptering medfører, vil stadig efterlade politiet stormskridt foran den situation, de var i for syv år siden, samtidigt med at alle andre bliver mere sikre over for myndigheders overreaktioner og kriminelle hackeres hærgen,« skriver han.

»De embedsmænd, der bruger så meget tid på at kritisere Apple, burde lægge den følelse af total berettigelse, som de har udviklet de seneste syv år, fra sig og bruge noget tid på at takke Apple og Google for at have gjort det så nemt for dem så længe«.

segj@information.dk

De mobile eller fastplacerede kameraer, som politiet gerne vil investere i, skal registrere nummerplader. Det vil bl.a. hjælpe politiet med at fange mange flere af de biler, der f.eks. ikke har været til syn, eller som ikke har en forsikring. Foto: Christian Klindt Sølbeck

Politidirektør: Overvågning af biler fanger mest små lovovertrædelser

Et nyt system til overvågning af biler via nummerplader er mest effektivt til at fange lovovertrædere som bilister, der ikke har fået synet deres bil. Politisk blev det oprindeligt sat i verden for at bekæmpe blandt andet grænseoverskridende kriminalitet

Af Mathias Koch Stræde

Den praktiske erfaring er indtil videre, at overvågning og genkendelse af nummerplader mestendels er effektivt i forhold til at fange mindre forseelser.

Det siger politidirektør Svend Larsen fra Rigspolitiet.

»Da vi kørte vores forsøg med systemet, var det i virkeligheden de helt banale forseelser, som vi fik langt, langt flest af. Når du har kameraet ude at køre i en politibil, så fanger du rigtig mange biler, der skulle have været til syn for et halvt år siden, hvor der ikke er blevet betalt afgift, eller hvor bilen ikke har en forsikring,« siger han. Men systemet er i første omgang tænkt til at blive brugt i en kamp mod tilrejsende udenlandske kriminelle, organiseret indbrudskriminalitet og hjemmerøverier. Det fremgår af den politiske flerårsaftale for politiet, som regeringen, Venstre, Konservative og Dansk Folkeparti indgik i slutningen af 2012. Rundt omkring i landet vil der således fra slutningen af næste år blive påbegyndt en opstilling af fastplacerede kameraer, der kan genkende nummerplader. Formentlig ved grænseovergange, broer og lignende steder. Derudover skal der installeres lignende kameraer til mobil brug i politibiler, som kan registrere andre forbipasserende køretøjer.

Begge typer kameraer skal genkende bilers nummerplader, så et system kan matche bilerne mod politiets lister med nummerplader af særlig interesse.

Men alle forbipasserende biler vil i udgangspunktet blive registreret, og politiet vil på den måde blive i stand til at indsamle data om, hvor mange tusinde biler er på et bestemt tidspunkt. I visse tilfælde vil der også blive taget et oversigtsbillede af hele køretøjet. Det er indtil videre de foreløbige planer for det såkaldte automatiske nummerpladegenkendelsessystem (ANPG), viser et notat fra Rigspolitiet til Datatilsynet, som Radio24syv tidligere har omtalt.

De mange for de få

Men systemet fanger også lidt større forseelser, forsikrer Svend Larsen fra Rigspolitiet.

»Det næste, vi får rigtig meget af, er stjålne nummerplader og biler. Det er jo hverken drabssager eller alvorlig narkokriminalitet. Men for mig at se er der på den måde ingen nedre grænse for, hvad man kan bruge systemet til. Der, hvor vi navnlig vil bruge det – og der, hvor kolleger, vi har talt med i udlandet, mener, at man kan bruge det – er de her småting,« siger Svend Larsen.

– Er det ikke et stort og indgribende system at sætte i gang i forhold til banal kriminalitet?

»Du kan også bruge det til mere alvorlige ting. Da vi fik pengene til det fra politikerne, var det jo tænkt til at begrænse grænseoverskridende kriminalitet og til en grænsekontrolsfunktion. Det får du også med systemet. Vi kan også bruge det, når vi fra Europol eksempelvis får underretninger om, at der er en bil på vej fra et østeuropæisk land,« siger Svend Larsen. Hele systemet kan karakteriseres som 'masseovervågning', vurderer Peter Blume, der er juraprofessor på Københavns Universitet med speciale i persondataret. Han argumenterer for, at det er et system, hvor man indsamler data om de mange for at finde de få.

»Det er også et godt eksempel på, at fordi teknologien gør overvågningen nemmere og nemmere, så kommer der også automatisk mere og mere overvågning,« siger Peter Blume. Men sådanne systemer er svære at argumentere imod: »Begreber som det private og det at kunne færdes i fred er noget ubestemmeligt noget, som typisk har det sværere over for mere hårdtslående argumenter som bekæmpelse af kriminelle. Men det er samtidig en del af den frihed, som er del af demokratiet,« siger han.

Gemmer i en måned

Et af de centrale spørgsmål, som kritikere af systemet har bragt frem, er, hvor lang tid de oplysninger, som systemet indsamler, skal gemmes.

Ifølge Rigspolitiets notat er udgangspunktet, at de data, som de indsamler – altså nummerplade, sted, tid og i visse tilfælde et oversigtsbillede – skal gemmes i 30 dage. Samtidig ønsker Rigspolitiet at gemme data i op til to år for de biler, hvis nummerplader matcher nummerplader på såkaldte hotlister. Planen er, at politiet selv skal genere disse hotlister ud fra eksempelvis registre over efterlyste køretøjer, manglende syn og forsikring.

Spørgsmålet er så, om politiet selv kan sætte nummerplader på disse hotlister, hvis de eksempelvis indgår i eller udviser et interessant kørselsmønster – som politiet har analyseret sig frem til ud fra de allerede indsamlede data. Hvis det bliver muligt, vil politiet opnå en slags 'cirkulær' adgang til at sætte de nummerplader på listerne, som de ønsker. Med andre ord kan overvågning blive grundlag for yderligere overvågning. Og så kan politiet potentielt omgå kravet om, at data i udgangspunktet skal slettes efter 30 dage. Det påpeger Jesper Lund, der er næstformand i IT-Politisk Forening.

»Jeg tror, at de prøver at strække opbevaringsperioden ud over de 30 dage,« siger Jesper Lund. Til den bekymring siger politidirektør Svend Larsen: »Det er netop sådan noget, Datatilsynet skal kigge på.« Han understreger, at Rigspolitiet stadig er i en dialog med Datatilsynet om, hvordan reglerne på området skal se ud.

»Hvis der ikke var nogen restriktioner på det her område, så er der ingen tvivl om, at vi ud fra en snæver politifaglig vinkel ville ønske at have så meget data som muligt. Og man ville ønske, at man kunne gemme det til evig tid,« siger Svend Larsen og fortsætter: »Men hensynet til politiets efterforskning skal afvejes i forhold til hensyn til privatliv og databeskyttelse. Og det er netop det, Datatilsynet skal gøre.«

maks@information.dk

Information

70. ÅRGANG | NR. 139 UAFHÆNGIG AF PARTIPOLITISKE OG ØKONOMISKE INTERESSER TORSDAG 19. JUNI 2014

Partnerskab med NSA

Leder

Indtil i dag har vi alene kendt historierne fra internationale medier. De seneste måneder er det løbende blevet dokumenteret, hvordan den amerikanske efterretningstjeneste NSA har opbygget et globalt netværk, der gør det muligt at masseovervåge almindelige borgeres tele- og internettrafik.

I dag kan Information placere Danmark direkte i det, der er blevet kaldt vor tids største historie om overvågning i åbne demokratier. Efter måneders research kan vi via whistlebloweren Edward Snowden give svar på nogle af de spørgsmål, der hidtil i den danske debat alene har været baseret på hypoteser og antagelser.

Denne avis har tidligere dokumenteret NSA's planer om at overvåge forhandlingerne under COP15 i Bella Center i 2009. I dag kan vi fortælle om Forsvarets Efterretningstjenestes (FE) placering i det globale netværk, der styres fra NSA's hovedkvarter i Fort Meade i USA. Et samarbejde, som NSA's daværende øverste chef Keith Alexander i 2012 betegnede som »det langvarige NSA-FE-partnerskab«.

Efter dagens artikler ved vi en del mere om Danmarks samarbejde med NSA, men der er fortsat meget, vi endnu ikke ved i en historie, hvis fulde omfang, dybde og perspektiv vi nok først langsomt vil forstå.

For ja, Danmark har efter alt at dømme et tæt og fortroligt samarbejde med NSA. Ja, NSA har ifølge dokumenterne formentlig adgang til tele- og internettrafik, der via såkaldte fiberkabler transporteres igennem Danmark. Ja, Danmark indgår tilsyneladende i et omfattende og internationalt ubeskrevet overvågningsprogram ved navn RAMPART-A, hvis globale rækkevidde offentligheden endnu ikke kender.

Og ja, det kan sagtens være helt rigtigt, når forsvarsminister Nicolai Wammen (S) og statsminister Helle Thorning-Schmidt (S) hidtil har udtalt, at »vi har ikke grund til at tro, at der er foregået ulovlige efterretningsaktiviteter mod Danmark eller danske interesser«.

Forelagt de dokumenter, Information i dag fremlægger, varierer forsvarsministeren sin forklaring ved at forsikre om, at alt, hvad der foregår, er lovligt.

Hvis det er tilfældet, bør det kalde på politisk debat og eftertanke. For i så fald har Folketinget vedtaget en lov, der åbner for en radikal form for massevervågning uden at gøre opmærksom på det i loven.

Præsident Barack Obama har gentagne gange advaret mod at offentliggøre dokumenter som dem, vi fremlægger i dag. Oplysningerne vil ifølge præsidenten i de forkerte hænder kunne kompromittere efterretningstjenesternes videre arbejde. I yderste instans vil de kunne bringe sikkerheden i fare for borgerne i den vestlige verden.

Vi er vores ansvar fuldt bevidst, men efter vores opfattelse bringer de fremlagte oplysninger hverken nationers eller personers sikkerhed i fare, fordi vi alene omtaler det overordnede samarbejde og ikke konkrete operationer eller personer.

Men vi medgiver, at oplysninger kan forekomme ubekvemme for såvel Barack Obama som Helle Thorning-Schmidt, der tydeligvis vil gå langt for at undgå en åben, demokratisk debat. Men på baggrund af dagens artikler synes der ingen vej uden om. Debatten om demokratisk kontrol med efterretningstjenesterne er afgørende for, at borgerne kan opretholde tilliden til dem, der har adgang til at kontrollere alle os andre.

> **Debatten om demokratisk kontrol med efterretningstjenesterne er afgørende for, at borgerne kan opretholde tilliden til dem, der har adgang til at kontrollere alle os andre**

Helle Thorning-Schmidt skylder nu svar på flere spørgsmål: Hvis der findes et partnerskab om adgang til fiberkabler mellem NSA og Forsvarets Efterretningstjeneste, hvorfor har regeringen så ikke blot lagt det åbent frem? Dermed ville ingen statshemmeligheder være røbet.

Hvis Danmark ikke har 100 procent kontrol over den tele- og internettrafik, NSA har adgang til via fiberkabler her i landet, hvorfor har regeringen så ikke forsøgt at sætte en stopper for det?

Det afgørende i denne sag er ikke nødvendigvis spørgsmålet om lovligt eller ulovligt. Mindst lige så afgørende er det, at vi i Danmark nu endelig får et mere oplyst grundlag for debatten om, hvor omfattende overvågning et åbent samfund kan acceptere uden selv at undergrave det åbne demokratis mest grundlæggende principper.

cj

FOLK

Ved Katrine Hornstrup Yde

Ulykkesfolk I

8.000 børn kommer til skade på trampoliner hvert år, viser nye tal, men 'ulykkerne er ikke så alvorlige, som vi har set tidligere', siger overlæge. Ungerne er altså blevet dårligere til at passe på, men bedre til at komme galt af sted med måde.

Ulykkesfolk II

Modsat er det med skuespillere. Sidste uge blev Harrison Fords ankel beskadiget under optagelserne til 'Star Wars'. Nu er Bodil Jørgensen blevet kvæstet under optagelserne til den kommende 'Far til fires vilde ferie'. Ulykken involverede en traktor.

Giftfolk

Henrettelse må helst ikke ske med måde. I april lå den dødsdømte morder Clayton Lockett, der først havde afventet sin henrettelse i 15 år, og rallede i 40 minutter, før han døde af et hjerteslag. Giften havde været for ringe.

Stædigfolk

Nu, efter otte ugers henrettelsespause, har USA genoptaget arbejdet med sprøjten, der jo trods alt erstatter den langt mere blodigt fejlslagne elektriske stol. Man må op på hesten igen. (Og tilbage på trampolinen, unger!)