JUSTITSMINISTERIET
Civil- og Politiafdelingen

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 26. maj 2009
Kontor: Politikontoret
Sagsnr.: 2009-157-0062
Dok.: AMC40808

Hermed sendes besvarelse af spørgsmål nr. 4 (B 105), som Folketingets Retsudvalg har stillet til justitsministeren den 24. februar 2009. Spørgsmålet er stillet efter ønske fra Anne Baastrup (SF).

Brian Mikkelsen

/

Barbara Bertelsen

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 4 (B 105) fra Folketingets Retsudvalg:

> ”Ministeren bedes hurtigst muligt og med bistand af ambassaderne i Sverige, Norge, Finland, Island, UK, Tyskland og Holland samt eventuelt andre særligt relevante lande gøre rede for, om personer og organisationer i disse lande kan få oplyst, om de er registreret af en efterretningstjeneste samt om praksis i disse lande for opbevaring og sletning af gamle oplysninger.”

Svar:

1. Justitsministeriet har til brug for besvarelsen indhentet oplysninger fra de norske myndigheder samt gennem Udenrigsministeriet fra de danske ambassader i Stockholm, Helsingfors, Reykjavik, London, Berlin og Haag.

2. Om forholdene i Sverige fremgår det af de indhentede oplysninger, at det svenske sikkerhedspoliti (SÄPO) som myndighed er underlagt offentlighedsprincippet. Udgangspunktet er derfor, at personer og organisationer skal kunne få indsigt i myndighedens virksomhed.

Dette udgangspunkt fraviges dog for så vidt angår oplysninger, der er underlagt den svenske fortrolighedslov (sekretesslagen). Er dette tilfældet, har sikkerhedspolitiet således ret til at undtage de pågældende oplysninger fra offentlighed. Det overlades til myndigheden selv at vurdere, hvorvidt oplysningerne skal udleveres inden for de gældende regler. Store dele af sikkerhedspolitiets virksomhed og arbejde er underlagt fortrolighed.

Den 1. januar 2008 oprettede Sverige en statslig myndighed (Säkerhets- och integritetsskyddsnämnden), som har til opgave at føre tilsyn med sikkerhedspolitiets behandling af oplysninger samt at påse, at sikkerhedspolitiets registre føres i overensstemmelse med lovgivningen. Nævnet fører tilsyn såvel ved henvendelse fra den enkelte borger som på eget initiativ.

Reglerne om politiets registre følger af polisdatalagen. Sikkerhedspolitiet må herefter ikke føre registre over personer udelukkende på baggrund af personens race, etniske oprindelse, politiske overbevisning, religiøse eller filosofiske tro, medlemskab i fagforening eller seksuelle præferencer. Disse oplysninger (følsomme personoplysninger) må kun behandles, hvis

det er uundgåeligt nødvendigt for behandlingens formål og i dette tilfælde kun som et tillæg til andre oplysninger.

Personer og organisationer har altid mulighed for at begære indsigt i sikkerhedspolitiets registre, hvorefter sikkerhedspolitiet behandler hver enkelt sag individuelt. I disse tilfælde vil oplysninger, som ikke er fortrolige, blive udleveret. Hvis en person har mistanke om, at sikkerhedspolitiets behandling af oplysninger ikke er i overensstemmelse med lovgivningen, er det altid muligt at henvende sig til Säkerhets- och integritetsskyddsnämnden.

Det følger af polisdatalagens § 35, at hovedreglen for opbevaring af oplysninger er 10 år. Hovedreglen kan i særlige tilfælde fraviges, således at oplysningerne opbevares i længere tid.

3. Om forholdene i Norge fremgår det af de indhentede oplysninger, at det norske forsvars efterretningstjeneste kan opbevare al information, som er tjenstlig relevant. Der er ingen regler om tidsbegrænsning.

Reglerne om Politiets Sikkerhetstjeneste (PST) findes i §§ 12-16 i instruksen for PST. Af § 13 fremgår, at PST kun kan anvende oplysninger til det formål, hvortil de er indhentet, samt til andre politimæssige formål og forvaltningsvirksomhed i tjenesten, medmindre andet er bestemt i lov eller i medfør af lov.

Det følger endvidere af § 13, at oplysninger kun må behandles af PST, hvis der ved oprettelse af en forebyggelsessag er grund til at undersøge, om nogen forbereder et strafbart forhold, som PST har til opgave at forebygge, eller det i øvrigt må anses for nødvendigt i forebyggelsesøjemed at behandle oplysninger af betydning for udførelsen af arbejdsopgaverne i politilovens § 17 b eller § 17 d, herunder oplysninger om udlændinge, hvis det efter en konkret sikkerhedsmæssig vurdering må anses for nødvendigt at behandle sådanne oplysninger. Tilsvarende kan PST også behandle oplysninger om referencepersoner i Norge for sådanne udlændinge.

Desuden må PST behandle oplysninger uden for straffesager, hvis behandlingen er nødvendig for tjenestens udarbejdelse af trusselvurderinger, for samarbejdet med andre landes politimyndigheder og sikkerheds- og efterretningstjenester eller for personkontrol eller akkreditering.

I den enkelte straffesag følger adgangen til at behandle oplysninger af reglerne i straffeproceslovens § 224 og § 226.

Instruksens § 14 indeholder krav til oplysningernes kvalitet. Således skal oplysninger, som behandles af PST, være tilstrækkelige og relevante for formålet med behandlingen, korrekte og opdaterede, ligesom oplysningerne ikke må opbevares længere, end formålet med behandlingen tilsiger.

§ 15 nævner en række personoplysninger, som ikke kan behandles af PST. Således kan oplysninger om en person ikke behandles kun på baggrund af oplysninger om personens etnicitet eller nationale baggrund, politiske, religiøse eller filosofiske overbevisning, fagforeningstilhørsforhold eller oplysninger om helbredsmæssige eller seksuelle forhold.

Efter § 16 skal chefen for PST sørge for at etablere et internt kontrolsystem, som bl.a. skal sikre oplysningernes kvalitet og varetage retssikkerhed og personbeskyttelse. PST skal udarbejde nærmere retningslinjer for behandling af oplysninger. Retningslinjerne skal godkendes af Justitsdepartementet.

Spørgsmålet om egenacess vedrører ifølge de norske myndigheder i praksis stort set kun PST.

Det er fast praksis, at PST hverken be- eller afkræfter, om tjenesten har registreret oplysninger om en person.

I forbindelse med klager herover til det såkaldte EOS-udvalg, som er et permanent parlamentarisk kontroludvalg, hænder det, at udvalget anmoder om samtykke fra tjenesten eller Justitsdepartementet til at give en mere fyldestgørende begrundelse, hvis der foreligger særligt behov herfor.

Forsvarets efterretningstjeneste vil ligeledes stort set aldrig hverken be- eller afkræfte en registrering.

4. De finske myndigheder har oplyst følgende om forholdene i Finland:

> ”Individuals and organizations in Finland cannot obtain information about their registration by the Finnish Security Police.

> According to the Personal Data Act (523/1999) the main rule is that regardless of secrecy provisions, everyone shall have the right of access, after having supplied sufficient search criteria, to the data on him/her in a personal data file, or to a notice that the file contains no such data. The controller shall at the same time provide the data subject with information of the regular sources of data in the file, on the uses for the data in the file and the regular destinations of disclosed data. However there is no aforementioned right of access, if providing access to the data could compromise national security, defence or public order or security, or hinder the prevention or investigation of crime.
>
> Furthermore according to the Act on the Processing of Personal Data by the Police (761/2003) the right of access does not apply in any way to data in the Operational Data System of the Security Police, but at the request of the data subject, the Data Protection Ombudsman may examine the lawfulness of the data that is held on the data subject.
>
> Data on a person held in the Operational Data System of the Security Police is deleted 25 years after the last data entry was made. Data in the data system concerning basic background checks and extended background checks is deleted within one year of conducting an equivalent new background check, but in any event no later than ten years after the check. After the deletion of the data, it cannot be used in the police work.
>
> The classified documents of the Security Police continue to be secret for 60 years pursuant to the Government decision and the transitional provision of the current Act on the Openness of Government Activities."

5. Om forholdene i Island fremgår det af de indhentede oplysninger, at problemet med hemmelige kartoteker ifølge de islandske myndigheder aldrig har været særligt stort i Island og aldrig er blevet debatteret på samme måde som i Danmark. Baggrunden for dette er bl.a., at man aldrig har haft særlige politiafdelinger som f.eks. PET i Danmark, PST i Norge eller SÄPO i Sverige.

Regulativ 322/2001 indeholder generelle forskrifter om, hvordan personoplysninger hos politiet skal behandles. Registrering af organisationer er ikke omtalt i regulativet. Ifølge regulativets artikel 2, litra 4, kan politiet oprette og føre personregistre "for at forhindre overhængende fare eller bekæmpe kriminalitet".

Artikel 10 om meddelelsespligt i forbindelse med indsamling af personoplysninger har i dansk oversættelse følgende ordlyd:

> ”Hvis personoplysninger er indsamlet og registreret uden den registreredes kendskab, skal man om muligt give den registrerede meddelelse om oplysningerne, hvis det ikke menes at forhindre politiets arbejde. Dette gælder ikke oplysninger, som er tilintetgjort.”

Artikel 13 omhandler destruktion af oplysninger:

> ”Er registrerede personoplysninger ikke længere nødvendige for politiets arbejde på grund af alder eller af andre grunde, skal de tilintetgøres.”

Endvidere er i samme artikel en bestemmelse om, at rigspolitichefen skal holde registernævnet orienteret om politiets registre.

6. Om forholdene i Storbritannien fremgår det af de indhentede oplysninger, at Home Office (Office for Security and Counter-Terrorism) har oplyst, at de britiske efterretningstjenester er undtaget fra reglerne i Freedom of Information Act og Data Protection Act om ret til indsigt i oplysninger, jf. i øvrigt nedenfor. Dette betyder, at personer og organisationer, der henvender sig til tjenesterne, ikke vil kunne få oplyst, hvorvidt de er registeret hos tjenesterne.

Home Office oplyser desuden, at reguleringen af tjenesterne findes i Security Service Act og Intelligence Service Act, der ikke regulerer spørgsmålet om opbevaring og sletning af oplysninger.

Home Office har endvidere oplyst følgende:

> ”In regard to the question concerning what information was disclosable to an individual if, for example, they were subject to a security service investigation the short answer is that the security service is exempt from disclosing information, including under the freedom of information act however, the relevant guidance and laws are listed below:
>
> - Security Service Act 1989 (this is the act that first acknowledged that the security service existed). This sets out the safeguards as well, such as warrants, reviews by the security service commissioner etc. http://www.opsi.gov.uk/ACTS/acts1989/Ukpga_19890005_en_1.htm.

- Intelligence Services Act 1994 (this is the act which acknowledged the other agencies – GCHQ and the Secret Intelligence Service, and sets our similar safeguards like warrants) http://www.opsi.gov.uk/ACTS/acts1994/ukpga_19940013_en_1.

- Freedom of Information Act – (part II sets out the exemptions, section 23 mentions the exemptions due to national security and specifically mentions the security agencies) http://www.opsi.gov.uk/Acts/acts2000/ukpga_20000036_en_1.

- Data Protection Act (sets out the role of the Information Commissioner and the Data Protection Tribunal). http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1.

Please note that a ruling in the tribunal by the Information Commissioner to disclose information can be overruled by a secretary of state (e.g. this has just been demonstrated in the case where the information commissioner ruled that cabinet minutes in the run up to the Iraq war should be disclosed, however, Jack Straw has recently overruled this to prevent disclosure. This step does have political ramifications)."

7. Om forholdene i Tyskland fremgår det af de indhentede oplysninger, at personer i henhold til den tyske Verfassungsschutzgesetz § 15 har ret til at søge om indsigt i registreringer hos Tysklands tre efterretningstjenester. Retten til indsigt gælder kun for individer, ikke for organisationer. Ansøgningen stiles til Bundesamt für Verfassungsschutz (BAV) (www.verfassungsschutz.de) i Köln.

Forudsætningerne for udlevering af oplysninger er, at vedkommende henviser til et konkret sagsforhold (f.eks. deltagelse i en demonstration), og at vedkommende har en særlig interesse i disse oplysninger (f.eks. grundet forestående ansættelse i det offentlige). Udlevering af oplysninger afslås i følgende fire tilfælde:

1. Hvis udleveringen af oplysningerne indebærer en fare for opgavevaretagelsen.
2. Hvis udleveringen bringer kilder i fare eller på anden måde sætter arbejdsmetoder hos og viden om Bundesamt für Verfassungsschutz over styr.

3. Hvis udleveringen bringer den offentlige sikkerhed i fare eller på anden måde medfører ulemper for Forbundsrepublikken eller for en eller flere delstater.
4. Hvis registreringer af hensyn til en tredjepart eller ifølge et særligt retsligt grundlag skal hemmeligholdes.

Oplysningspligten strækker sig ikke til informationer om registreringernes oprindelse eller modtagere. Afvises ansøgningen, skal BAV oplyse, hvilke forhold der ligger til grund for afslaget.

For så vidt angår praksis for opbevaring og sletning kan det oplyses, at der skelnes mellem, om registreringerne foreligger i elektronisk form eller på papir.

Elektroniske data opbevares som hovedregel i 10 år, registreringer vedrørende terrorisme dog i 15 år. Efter fristens udløb afgøres det, om der er behov for at opbevare registreringerne yderligere. Hvis dette ikke er tilfældet, slettes de.

Oplysninger på papir er i princippet underlagt samme slettefrister som elektroniske data. Dog kan man – frem for at destruere – vælge at spærre særlige akter og markere dem som ikke-tilgængelige.

8. Om forholdene i Nederlandene fremgår det af de indhentede oplysninger, at personer og organisationer generelt har adgang til at få indsigt i personlige og øvrige oplysninger indsamlet af de nederlandske efterretningstjenester, jf. lov om efterretnings- og sikkerhedstjenester (herefter efterretningsloven) af 2002. Formen for sådan aktindsigt kan variere alt efter oplysningernes karakter, men omfatter fysisk inspektion af akterne ved efterretningstjenesterne, modtagelse af kopi af relevante akter og udarbejdelse af resumeer af relevant information.

Den relevante minister (henholdsvis indenrigsministeren og forsvarsministeren) skal som hovedregel inden for tre måneder efter en anmodning om indsigt oplyse ansøgeren om, hvorvidt oplysninger er blevet behandlet af efterretningstjenesterne og i givet fald hvilke.

Retten til sådan aktindsigt gælder dog generelt ikke, hvis:

- oplysningerne er fremkommet som led i en efterforskning og er yngre end fem år gamle,

- der i mellemtiden er fremkommet yderligere information i relation til den efterforskning, der frembragte de oprindelige oplysninger,
- oplysningerne er relevante for en igangværende efterforskning.

Oplysninger kan ligeledes undtages af hensyn til kongerigets enhed (”unity of the Crown”), statens sikkerhed, forholdet til fremmede magter og organisationer, statens økonomiske interesser, hensynet til individers privatliv og lignende. Afslag på aktindsigt skal i disse tilfælde meddeles en uafhængige kontrolkomité (CTIVD).

Der er i efterretningsloven fastsat regler for sletning og overførsel af oplysninger. Generelt skal oplysninger fjernes, så snart disse ikke længere har meningsværdi i relation til det formål, hvortil de er indhentet. Sletning er dog underlagt de begrænsninger, som måtte følge af anden offentlig arkivlovgivning.

Det har ikke været muligt at indhente nærmere oplysninger om praksis for opbevaring og sletning af efterretningsoplysninger.