



Remiss av departementspromemorian *Behandling av personuppgifter inom Nationellt centrum för terrorhotbedömning (Ds 2016:31)*
(Ju2016/06351/L4)

Juridiska fakulteten vid Uppsala universitet har genom remiss anmodats att avge yttrande i rubricerat ärende. Juridiska fakultetsnämnden välkomnar i stort promemorians förslag om kompletterande bestämmelser för behandling av personuppgifter inom Nationellt centrum för terrorhotbedömning, NCT, men finner att en fördjupad utredning bör göras i centrala frågor.

Bakgrund

Promemorian utreder behandlingen av personuppgifter som sker inom NCT, ett samarbetsorgan som involverar Säkerhetspolisen, Försvarets radioanstalt (FRA) och Militära underrättelse- och säkerhetstjänsten (MUST). Utredningen har föranletts av att två av de organ som är satta att övervaka de inblandade organen, Statens inspektion för försvarsunderrättelseverksamhet (SIUM) och Säkerhets- och integritetsskyddsnämnden (SIN) i skilda rapporter funnit att det råder osäkerhet vad gäller regleringen av myndigheternas personuppgiftsansvar, samt vad gäller vissa sekretessfrågor.

Direktåtkomst

I promemorian läggs förslag om att de inblandade myndigheterna ska få dela uppgifter ur sina uppgiftssamlingar med varandra genom direktåtkomst, vilket möjliggörs genom att uttryckliga regler härom införs i respektive myndighet regelverk för personuppgiftsbehandling (se särskilt s. 170-185). SIN kom i sitt yttrande (se ovan) fram till att nuvarande utbyte av personuppgifter inte är av omfattande karaktär. Genom att tillåta direktåtkomst kan förväntas att mer, eller betydligt mer personuppgifter kan komma att överföras mellan myndigheter. Förutsättningarna ändras därmed, vilket även innebär ett utökat behov av kontroll av verksamheten. Frågor om ansvarsutkrävande och kontroll behandlas nedan.

Därtill kan ifrågasättas promemorians slutsats att direktåtkomst inte medför några problem i sak, då alla myndigheter har någorlunda överensstämmande regler om personuppgiftsbehandling (se s. 140-141) och har lika långtgående sekretesskrav (s.176). Verksamheten hos de inblandade myndigheterna skiljer sig dock åt. Säkerhetspolisen håller på med brottsbekämpning, de andra två myndigheter med mer renodlat underrättelsearbete. Förutsättningarna för att samla in uppgifter kan förväntas skilja sig åt. FRA och MUST övervakar



externa hot, varför trösklarna för registrering av personer kan förväntas vara lägre för FRA och MUST än för Säkerhetspolisen. Även om reglerna är desamma, finns det därför risk att mer "löst grundad" informationen kommer in i Säkerhetspolisens system och blir behandlat på ett liknande sätt som Säkerhetspolisens övriga information, vilken (antagligen) är mer grundad. Fakultetsnämnden saknar en grundlig utredning av denna centrala fråga. Utredningen föreslår att ordet "strategisk" skrivs in i de föreslagna förordningarna för att ha en begränsande effekt på informationsutbytet (s. 180), men gränsdragning mellan "strategisk" och "taktiskt" är svävande. Övriga "spärrar" i systemet är interna, huvudsakligen att anställda inom en myndighet får elektroniskt tillgång endast till de personuppgifter som de behöver i sitt arbete (s. 176). Allmänheten har dock ingen insikt i om, eller hur, sådana interna kontroller fungerar. Som minimum bör de externa tillsynsorganen (SIN och SIUN) uppmärksamhet riktas på dessa frågor, och deras resurser förstärkas.

Fakultetsnämnden anser att utredningen inte tillräckligt belyst konsekvenserna av det lagda förslaget och avstyrker förslaget i denna del.

Delegation

Sedan tidigare kan regeringen genom förordning meddela ytterligare föreskrifter om vilka myndigheter som får ha direktåtkomst till uppgiftssamlingarna, en regel som här enbart föreslås ändras i språkligt hänseende. Mot bakgrund av att de myndigheterna som är involverade i NCT nu anges uttryckligen i det föreslagna lagrummet, kan regeln om ytterligare myndigheter uppfattas som att regeringen på egen hand kan utvidga kretsen av myndigheter som kan få direktåtkomst till de inblandade myndigheternas uppgiftssamlingar till ett obestämt antal myndigheter. Promemorian innehåller inte någon närmare diskussion vilka dessa ytterligare myndigheter skulle kunna vara. Eftersom det är fråga om potentiellt ytterst känsliga uppgifter, och att regeln inte innehåller någon begränsning av vilka myndigheter som kan tillåtas få direktåtkomst, förefaller det vara en alltför långtgående delegation av normgivningskompetens. Skyddet för den personliga integriteten i RF 2:6 andra stycket jämförd med RF 2:20 motiverar att lagform används. I promemorian anges vidare (s. 209) att även myndigheter som regeringen bestämmer skulle kunna meddela ytterligare föreskrifter om vilka myndigheter som får ha direktåtkomst. Detta har inte någon täckning i de föreslagna lagrummen, men fakultetsnämnden vill likväl framhålla att en sådan långtgående delegation är direkt olämplig.

Fakultetsnämnden avstyrker förslaget vad gäller utformningen av delegation av normgivningskompetens till regeringen i denna del.

Sekretess

För att möjliggöra att sekretessbelagda uppgifter kan utlämnas, införs vidare en sekretessbrytande bestämmelse i form av en uppgiftsskyldighet. Fakultetsnämnden anser att förslaget innebär en tillräckligt tydlig reglering av sek-



retessfrågan och tillstyrker, för det fall direktåtkomst kan anses lämpligt, förslaget i denna del.

Oklar reglering för det gemensamma personuppgiftsansvaret

Promemorian anser inte att det finns anledning att införa särskilda regler för det gemensamma personuppgiftsansvar som de inblandade myndigheterna utövar inom ramen för NTC. Istället föreslås att de otydligheter som kan följa med det gemensamma personuppgiftsansvaret ska regleras via en överenskommelse mellan myndigheterna.

Fakultetsnämnden vill i sammanhanget understryka att EU-rätten innehåller krav vad gäller såväl form som innehåll för den reglering som grundar rätt att behandla personuppgifter utan samtycke. Av målet C-201/14 Smaranda Bara m.fl.¹, som rör dataskyddsdirektivet 95/46/EG, följer att den rättsliga grunden behandlingen måste regleras i "lagstiftning", samt att icke-publicerade protokoll med en överenskommelse mellan myndigheter inte är tillräcklig. I förevarande fall regleras som framgått ovan själva utlämnandet av uppgifter i myndigheternas regelverk för personuppgiftsbehandling, varför detta krav är uppfyllt. I den nya dataskyddsförordningen 2016/679, som ska tillämpas från den 25 maj 2018, stipuleras vidare vissa specifika krav för hur ett gemensamt personuppgiftsansvar ska regleras. Enligt artikel 26 punkten 1 i dataskyddsförordningen anges att, såvida inte de personuppgiftsansvarigas respektive skyldigheter fastställs i antingen EU-rätten eller tillämplig nationell rätt, ska gemensamt personuppgiftsansvariga "under öppna former fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt denna förordning, särskilt vad gäller utövandet av den registrerades rättigheter och sina respektive skyldigheter att tillhandahålla den information som avses i artiklarna 13 och 14 (rörande information som den registrerade har rätt till) genom ett inbördes arrangemang". Vidare anges i punkten 2 arrangemanget på lämpligt sätt ska återspegla de gemensamt personuppgiftsansvarigas respektive roller och förhållanden gentemot registrerade, samt att det väsentliga innehållet i arrangemanget ska göras tillgängligt för den registrerade. I punkten 3 anges att oavsett formerna för det arrangemang som avses i punkt 1 får den registrerade utöva sina rättigheter enligt förordningen med avseende på och emot var och en av de personuppgiftsansvariga. Av punkt 79 i preambeln till dataskyddsförordningen understryks att gemensamt personuppgiftsansvar kräver ett tydligt fastställande av vem som bär ansvaret enligt förordningen, även i förhållande till tillsynsmyndigheternas övervakning och åtgärder.

Av detta följer att EU-rätten inte kräver att det gemensamma personuppgiftsansvaret regleras genom lagstiftning, men att de "inbördes arrangemang" som reglerar det gemensamma ansvaret måste uppfylla de krav som anges i artikel 26 i dataskyddsförordningen. Promemorian innehåller inte någon ut-

¹ Mål C-201/14 Smaranda Bara et al mot Președintele Casei Naționale de Asigurări de Sănătate, EU:C:2015:638



trycklig analys av hur dessa krav kan uppfyllas i den överenskommelse som föreslås ingås av de inblandade myndigheterna.

Liknande synpunkter kan framföras så vitt gäller EKMR. Promemorian innehåller (s. 53-54) en mycket kort och summarisk genomgång av EKMR och Europadomstolens praxis. Ytterligare praxis bör uppmärksammas, särskilt rättsfallet *Shimovolos v. Russia*.² Fakultetsnämnden återger de viktiga paragraferna nedan (fakultetsnämndens fetstil).

1. The Court reiterates in this connection that in the special context of secret measures of surveillance the above requirements cannot mean that an individual should be able to foresee when the authorities are likely to resort to secret surveillance so that he can adapt his conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on the application of secret measures of surveillance, especially as the technology available for use is continually becoming more sophisticated. The law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to any measures of secret surveillance **and collection of data**. In addition, because of the lack of public scrutiny and the risk of abuse intrinsic to any system of secret surveillance, the following minimum safeguards should be set out **in statute law** to avoid abuses: the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law (see *Uzun*, cited above, §§ 61-63; *Association for European Integration and Human Rights and Ekimdzhev v. Bulgaria*, no. 62540/00, §§ 71-77, 28 June 2007, *Liberty and Others v. the United Kingdom*, no. 58243/00, § 62, 1 July 2008, and, *mutatis mutandis*, *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 95 and 96, 4 December 2008).

2. Turning to the present case, the Court observes that the creation and maintenance of the Surveillance Database and the procedure for its operation are governed by ministerial order no. 47 (see paragraph **Fel! Hittar inte referenskölla**. above). That order is not published and is not accessible to the public. The grounds for registration of a person's name in the database, the authorities competent to order such registration, the duration of the measure, the precise nature of the data collected, the procedures for storing and using the collected data and the existing controls and guarantees against abuse are thus not open to public scrutiny and knowledge.

3. For the above reasons, the Court does not consider that the domestic law indicates with sufficient clarity the scope and manner of exercise of the discretion conferred on the domestic authorities to collect and store in the Sur-

² *Shimovolos v. Russia*, Application no. 30194/09 21 June 2011.



veillance Database information on persons' private lives. In particular, it does not, as required by the Court's case-law, set out in a form accessible to the public any indication of the minimum safeguards against abuse. The interference with the applicant's rights under Article 8 was not, therefore, "in accordance with the law".

Detta rättsfall stärker argumentet att huvudprinciperna i reglering bör ges i lag form. Som ovan angetts förutsätter även regeringsformen att det skydd för den personliga integriteten som garanteras i RF 2:6 andra stycket jämförd med RF 2:20 regleras genom lag.

Transparens, överblickbarhet och förutsättningar för ansvarsutkrävande
Fakultetsnämnden vill även peka på ett allmänt rättsstatligt behov av en transparent och överblickbar reglering av personuppgiftsbehandling, inte minst på grund av behandlingen inom området potentiellt kan vara mycket integritetskränkande för enskilda. Den fråga som innevarande promemoria behandlar avser ett komplext samarbete mellan flera inblandade myndigheter och övervakningsorgan, nämligen ett samarbetsorgan, NCT, som berör Säkerhetspolisen, FRA och MUST, samt övervakningsorganen Datainspektionen, SIN och SIUN. Den överlappande och splittrade regleringen av området innebär i sig en inte obetydlig svårighet för såväl övervakningsorganen själva som riksdagen att följa verksamheten. Härmed försvåras även förutsättningarna för ansvarsutkrävande. Redan detta förhållande talar för ett behov av en tydlig reglering av myndigheternas inbördes och gemensamma personuppgiftsansvar. I avsaknad på specifik reglering av det sistnämnda, vill fakultetsnämnden understryka vikten av att regering och riksdag tillser att den föreslagna överenskommelsen för gemensamt personuppgiftsansvar utformas på så sätt att såväl dataskyddsförordningens krav, EKMR:s som allmänt rättsstatliga krav på transparent och överblickbar reglering av personuppgiftsbehandling inom terrorhotbedömning uppfylls.

Ovan har konstaterats att en förslaget kan medföra en utökad delning av personuppgifter mellan myndigheter med olika uppgifter och syfte. Genom samarbetet i NCT kan således uppgifterna av annan kvalitet än vad som vanligen förekommer i respektive myndighets ordinarie verksamheten komma att behandlas. Önskemålet att reglera området på ett teknikneutralt sätt är förståeligt. Någon sammanhållen kontroll av verksamheten finns dock inte, utan verksamheten ska även fortsättningsvis övervakas av tre skilda myndigheter, DI, SIN, och SIUN. Mot bakgrund härav är det än viktigare PDL och de övriga lagarna, samt tillsyn av dessa, är utformat så enkelt och tydligt som möjligt. Regleringen i dess nuvarande utformning är svårtillgänglig även för experter inom ämnet, och kan förväntas vara än mindre tillgänglig för den bredare allmänheten. En bristande insikt och förståelse för hur systemet är uppbyggt kan i sig vara problematiskt, eftersom det riskerar undergräva allmänhetens förtroende och tillit. För att övervakningen ska uppfattas som försvarlig bör förutsättningarna för kontroll och ansvarsutkrävande vara tyd-



UPPSALA
UNIVERSITET

REMISSYTTRANDE

6 (6)

2016-12-16

JURFAK 2016/63

liga. En fördjupad analys av hur de föreslagna förändringarna inverkar på förutsättningarna för ansvarsutkrävande hade därför varit välkommen.

Förslag till yttrande i detta ärende har upprättats av professor Iain Cameron och professor Jane Reichel. Yttrandet har på delegation avgivits av fakultetens dekanus, professor Mattias Dahlberg.

A handwritten signature in black ink, appearing to read 'Mattias Dahlberg'.

Mattias Dahlberg