

Bemærkninger til betænkning nr. 1504/2009 om restaurationsers adgang til identitetsoplysninger på personer med restaurationsforbud

Justitsministeriet
Civil- og politiafdelingen
E-mailes til jm@jm.dk

18. august 2009, j.nr. 540.30/21294

Høring over betænkning nr. 1504/2009 om restaurationsers adgang til identitetsoplysninger på personer med restaurationsforbud

Justitsministeriet har med e-mail af 18. juni 2009 anmodet om en udtalelse over betænkning nr. 1504/2009 om restaurationsers adgang til identitetsoplysninger på personer med restaurationsforbud, jf. herved restaurationslovens § 31, stk. 2.

1. Baggrund

Det sagkyndige udvalg bag betænkningen har haft til opgave at foretage en samlet gennemgang og vurdering af, hvordan restaurationser mv. sikres adgang til identitetsoplysninger på personer med restaurationsforbud, uden at en sådan adgang til personfølsomme oplysninger om enkeltpersoner sætter grundlæggende hensyn til persondatabeskyttelsen over styr. Samtidigt er udvalget anmodet om at overveje mulighederne for at registrere personer, der er meddelt restaurationsforbud, i et særskilt register, som i fornødent omfang kan stilles til rådighed for restaurationser og dørmænd mfl. Der henvises til beslutningsforslag nr. B 112 (Folketingstidende 2006-07, Tillæg B, side 1783).

Betænkningen anbefaler bl.a.,

- a. ensretning af politiets underretningsprocedurer vedrørende meddelelse af restaurationsforbud samt ensretning af politiets praksis vedrørende meddelelse af sådanne til restauratører,
- b. klar lovhjemmel til at politiet kan videregive oplysninger om restaurationsforbud til nærmere angivne personer tilknyttet den relevante restauration samt regler om tavshedspligt vedrørende sådanne oplysninger, og
- c. oprettelse af et centralt privat register, hvor de restaurationsvirksomheder, som ønsker det, on-line kan få oplyst, om en bestemt person har restaurationsforbud det pågældende sted. Oplysninger vil blive meddelt efter søgning på "hit – no hit" ("ja/nej") basis, og restaurationsvirksomheden vil alene kunne få oplyst, om den pågældende person har forbud mod at opholde sig i den konkrete restauration. Det vil derfor ikke være muligt elektronisk at udveksle oplysninger om forbud, karantæne mv., svarende til et "Bølleregister" ("advarselsregister"), hvor oplysninger frit kan udveksles mellem restauranterne, typisk natklubber og diskoteker[1].

I det følgende afsnit behandles punkterne a. og b. sammen i afsnit 2.2, mens punkt c. behandles nedenfor under afsnit 2.3. Instituttets overordnede konklusion fremgår af afsnit 2.1 umiddelbart nedenfor. I afsnit 3. behandles ligebehandlingsmæssige konsekvenser.

2. Instituttets vurdering

2.1 Overordnet konklusion

- Instituttet tiltræder udvalgets anbefaling af ensretning af politiets underretningsprocedurer vedrørende meddelelse af restaurationsforbud samt ensretning af politiets praksis vedrørende meddelelse af sådanne til restauratører
- Instituttet tiltræder anbefalingen af, at der etableres klar lovhjemmel til, at politiet kan videregive oplysninger om restaurationsforbud til nærmere angivne personer tilknyttet den relevante restauration samt regler om tavshedspligt vedrørende sådanne oplysninger
- Udvalgets anbefaling af et privat, centralt register har primært sin årsag i, at et sådant register vil kunne indeholde billeder, templates (en matematisk værdi af et fingeraftryk) og andre oplysninger, som kan anvendes til en hurtig, ensartet og effektiv adgangskontrol. Disse oplysninger vil ikke kunne registreres i et centralt offentligt register uden lovændringer. Registrering af fingeraftryk, fotos mv. forudsætter udtrykkeligt samtykke fra den enkelte gæst. Instituttet finder, at det nærmere bør undersøges, om oprettelsen af et centralt, privat register er nødvendig og proportional, henset til den øgede registrering, som må forventes, og de datasikkerhedsmæssige betænkeligheder et sådant register rejser.
- Oprettelsen af et centralt, privat register rejser ikke særlige ligebehandlingsmæssige problemer, idet ordningen forudsættes administreret ens over for alle restaurationsgæster. Det kan således ikke udelukkes, at et register endog kan have en vis positiv effekt i relation til at mindske usaglig forskelsbehandling.

2.2 Bemærkninger i forhold til betænkningens anbefalinger vedrørende de under afsnit 1 nævnte punkter a. og b. om ensretning af politiets procedurer, klar lovhjemmel vedrørende videregivelse af oplysninger om forbud samt regler om tavshedspligt

Personoplysninger, herunder videregivelse og anden behandling af oplysninger om enkeltpersoners private forhold, hører ind under artikel 8 i Den Europæiske Menneskerettighedskonventionens (EMRK) beskyttelsesområde. Som også nævnt i betænkningen s. 43 vil videregivelse af sådanne oplysninger kun kunne ske på de betingelser, der er nævnt i artikel 8, stk. 2.

Statens mulighed for at begrænse eller påvirke adfærd forudsætter opfyldelse af de tre indgrebsbetingelser, der er nævnt i bestemmelsens stk. 2:

- legalitetskravet
- anerkendelsesværdige formål, der kan begrunde indgreb fra offentlige myndigheder i de beskyttede rettigheder
- kravet om nødvendighed i et demokratisk samfund.

Legalitetskravet betyder, at indgrebet skal have klar og sikker hjemmel. Opfyldelse af nødvendighedskravet forudsætter, at staten kan påvise, at der med indgrebet opnås en "fair balance" mellem borgerens rettigheder og samfundets modstående interesse i at begrænse vedkommende borgers rettigheder. Et indgreb skal kunne anses som "nødvendigt i et demokratisk samfund" eller begrundet i et påtrængende samfundsmæssigt behov. Heri ligger, at det ikke er tilstrækkeligt, at indgrebet er nyttigt, rimeligt og ønskeligt, eller fremstår som resultatet af et rimeligt og forsigtig skøn, udøvet i god tro. Omvendt kræver det ikke, at indgrebet er uomgængeligt nødvendigt. Den Europæiske Menneskerettighedsdomstol har udtrykt det således, at indgrebet må være "justified in principle – that is, whether the reasons adduced to justify them appear "relevant and sufficient" and are proportionate to the legitimate aim pursued"[2]. Staten er overladt en skønsmargin ("margin of appreciation") ved vurderingen af, om et indgreb er nødvendigt efter en national målestok. Proportionalitetskravet indebærer, at det middel, der bringes i anvendelse, skal være det mindre indgribende af flere muligheder og stå i et rimeligt forhold til det mål, som søges opnået.

Det er Institutets opfattelse, at der i videst muligt omfang bør tilstræbes klar og præcis lovgivning og en ensartet praksis ved administrationen af regler på områder, som vedrører indgreb i personers ret til respekt for privatliv, jf. herved EMRK artikel 8. Reguleringen af behandlingen af personoplysninger fremgår af persondatalovens regler, og af persondatalovens § 8, stk. 1, fremgår bl.a., at oplysninger, som vedrører strafbare forhold som udgangspunkt er undergivet hemmeligholdelse. Oplysninger om restaurationsforbud er derfor en fortrolig oplysning, da et sådant forudsætter, at vedkommende enten er sigtet for eller har begået et strafbart forhold.

Instituttet tiltræder de anbefalinger, som er indeholdt under punkterne a. og b. Særligt finder Instituttet det af afgørende betydning, at der tilvejebringes klar lovhjemmel vedrørende videregivelse af restaurationsforbud og nærmere regler om tavshedspligt om samme. Det kunne i den forbindelse overvejes, om forslaget til ny § 3, stk. 3 bør ændres således, at ordene "kan videregive" ændres til "videregiver", idet en sådan videregivelse er forudsætningen for, at restauratører kan medvirke til at håndhæve forbuddene gennem adgangskontrol mv.

Instituttet finder det samtidigt vigtigt at understrege, at der ved meddelelse af et restaurationsforbud altid skal foretages en konkret og selvstændig vurdering af, om et forbud er nødvendigt og proportionalt, se herved bl.a. Justitsministeriets cirkulæreskrivelse nr. 10092 af 21/12/2006[3].

2.3. Oprettelse af et centralt, privat register

En oplysning om, at en person har fået et restaurationsforbud er – som også nævnt ovenfor – en oplysning om strafbart forhold.

Europarådets konvention om persondatabeskyttelse[4] indeholder i art. 6 en begrænsning i adgangen til at videregive personoplysninger om strafbare forhold. Den lyder:

"Art 6. Personoplysninger vedrørende race, politisk overbevisning, religiøs eller anden trobekendelse, såvel som personoplysninger om helbred og seksuelle forhold, må ikke behandles elektronisk, medmindre national gældende lovgivning yder fornøden beskyttelse. Det samme gælder personoplysninger vedrørende straffedomme."

Borgerens ret til beskyttelse af personoplysninger om strafbare forhold er også omfattet af EU's Persondatadirektiv (95/46/EC)[5], som i art. 8, stk. 5 fastslår:

"Stk. 5. Behandling af oplysninger om lovovertrædelser, straffedomme eller sikkerhedsforanstaltninger må kun foretages under kontrol af en offentlig myndighed, eller hvis der gælder tilstrækkelige, specifikke garantier i medfør af den nationale lovgivning med forbehold af de undtagelser, som medlemsstaten kan fastsætte på grundlag af nationale lovbestemmelser, hvorefter der gives tilstrækkelige, specifikke garantier. Et fuldstændigt register over straffedomme må dog kun føres under kontrol af en offentlig myndighed.

....".

Direktivet har været bestemmende for udformningen af den danske persondatalov. Afgørende er, at indsamling og registrering sker til udtrykkeligt angivne og saglige formål, se hertil persondatalovens § 5, stk. 2. Formålet skal således defineres med en vis præcision, således at der skabes klarhed og åbenhed omkring behandlingen af relevante persondata. Videregivelse og behandling af oplysninger om enkeltpersoners rent private forhold, herunder strafbare forhold, er reguleret i persondatalovens §§ 7 og 8. Det følger bl.a. af § 8, stk. 2, nr. 1, at videregivelse kan ske, hvis den registrerede har givet sit udtrykkelige samtykke til sådan. § 8 bestemmer endvidere følgende i:

”Stk. 4. Private må behandle oplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold end de i § 7, stk. 1, nævnte, hvis den registrerede har givet sit udtrykkelige samtykke hertil. Herudover kan behandling ske, hvis det er nødvendigt til varetagelse af en berettiget interesse og denne interesse klart overstiger hensynet til den registrerede.

Stk. 5. De i stk. 4 nævnte oplysninger må ikke videregives uden den registreredes udtrykkelige samtykke. Videregivelse kan dog ske uden samtykke, når det sker til varetagelse af offentlige eller private interesser, herunder hensynet til den pågældende selv, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse.”

Persondatalovens § 7, stk. 1, vedrører oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbreds- og seksuelle forhold. En behandling som nævnt ovenfor i § 8 forudsætter, at der i hvert enkelt tilfælde, hvor den private skal behandle oplysninger, foretages en konkret vurdering af de nævnte hensyn.

Det fremgår af betænkningen bl.a. s. 12 og 85, at anbefalingen af et privat, centralt register primært har sin årsag i, at et sådant register – ud over identitetsoplysninger (navn og CPR-nummer på personer med restaurationsforbud) – også vil kunne indeholde billeder, templates (en matematisk værdi af et fingeraftryk) og andre oplysninger, som kan anvendes til en hurtig, ensartet og effektiv adgangskontrol. En sådan registrering vil ikke kunne ske i et centralt offentligt register, idet et sådant vil skulle baseres på CPR-numre, se f.eks. betænkningen s. 11. Registrering af fingeraftryk, fotos mv. forudsætter samtykke fra den enkelte gæst, jf. herved lovens § 3, nr. 8, om informeret samtykke og § 38 om tilbagekaldelse. Registret vil også kunne anvendes til at registrere oplysninger om intern karantæne, se betænkningen f.eks. s. 12 og 13.

Efter Institutets opfattelse rejser oprettelsen af et sådant register flere principielle spørgsmål

a. Proportionalitets- og nødvendighedsvurderinger

Udgangspunktet ved indsamling og registrering af persondata er, at kun oplysninger, som er relevante og tilstrækkelige og kræves til opfyldelse af de formål, hvortil oplysningerne indsamles og behandles, må indsamles, se hertil persondatalovens § 5. Den såkaldte ”Artikel 29-gruppe”, som er nedsat i medfør af databeskyttelsesdirektiv 95/46/EC, har omkring brugen af biometriske oplysninger bl.a. udtalt, at oplysninger, som opbevares i databaser, herunder fingeraftryk (templates), ”should be carefully assessed before such applications are put in place.”[6] Artikel 29-gruppen har samtidigt udtrykt betænkeligheder omkring den omfattende brug af fingeraftryk til personidentifikation i forbindelse med adgang til både fysiske og virtuelle områder, jf. herved følgende: ”A specific concern related to biometric data is that the public may become desensitised, through the widening of the use of such data, to the effect their processing may have on daily life.”[7].

Oprettelse af et privat, fælles register må efter Institutets opfattelse forventes at medføre en markant stigning i registreringen af biometriske oplysninger i form af fingeraftryk og personfotos. Restauranter, som ønsker at anvende registret, forudsættes at indhente disse oplysninger fra alle gæster. Dette forhold rejser spørgsmål i

relation til nødvendighed og proportionaliteten af at indsamle disse data fra "almindelige" gæster (uden restaurationsforbud). Udvalget nævner således også s. 60 i betænkningen, at der skal være tale om en afbalanceret og retssikkerhedsmæssig forsvarlig løsning, herunder at der ikke bør foretages en unødvendig (vores udhævning) registrering og overvågning af restaurationsgæster i nattelivet.

- Diskoteker/natklubber mv. har efter Datatilsynets afgørelse i Crazy Daisy-sagen allerede nu en adgang til at indsamle personoplysninger til brug for registrering af deres gæster med disses samtykke. Datatilsynet har i forbindelse med Crazy Daisy-sagen endvidere udtalt, at diskoteket uden samtykke kan indsamle, registrere og bruge oplysninger om restaurationsforbud, herunder personnummer på sådanne personer. Der er således adgang til en registrering af disse oplysninger, og formålet er derfor til dels allerede nu opfyldt. Samtidigt må det antages, at diskotekskæders gæsteregistreringssystemer i dag tillige fungerer som en form for "advarselsregister". Denne funktion kan et centralt, privat register ikke opfylde med det foreliggende forslag.
- På baggrund af den allerede eksisterende adgang til registrering, er det vigtigt, at "gevinsten" ved et centralt register i et vist omfang nærmere dokumenteres i relation til det overordnede formål: et tryggere natteliv. Det er således ikke tilstrækkeligt, at restauratørerne "slipper for" selv at registrere de personer, som har forbud mod at komme på restauranten, se betænkningen s. 11. Registret skal have en selvstændig funktion i relation til at "betrygge nattelivet", når dette sammenlignes med alternativer, herunder en decentral løsning.
- Oprettelsen og den løbende drift af registret må forventes at være ganske bekostelig og en delvis finansiering vil muligt ske via det offentlige. Også af denne årsag bør det afklares, om der er et reelt behov for et register af den nævnte karakter. Det kan ikke udelukkes, at store diskoteker, natklubber mv. foretrækker egne, mere detaljerede gæsteregistreringssystemer, og at mindre restaurationer foretrækker den enkle og billige løsning, hvorefter restaurationen selv administrerer et af politiet meddelt restaurationsforbud. Tilslutning til et fælles, centralt register må også antages at skulle anmeldes til Datatilsynet.
- Et privat centralt register rejser store databehandlingsmæssige udfordringer, jf. nærmere nedenfor, afsnit b. Risikoen for datamisbrug, dataudslip mv. må anses for at være ganske betydelig.

Det er på denne baggrund Instituttets opfattelse, at det grundigt bør overvejes, om der er et reelt behov for et sådant centralt register. Alternativt kunne det overvejes, om biometriske oplysninger kan lægges ind i et "gæstemicrochip-kort" eller lignende, således at lagring af større mængder af biometriske oplysninger i databaser i videst muligt omfang søges undgået.

b. Datasikkerhedsmæssige udfordringer

Artikel 29-gruppen har ved flere lejligheder understreget, at der gælder skærpede sikkerhedskrav ved registrering, behandling mv. af biometriske data, og det er bl.a. anført, gruppen " ... would point out that the growing interest in the application of biometric identification techniques calls for an extremely careful analysis of the legality of processing such data for identification purposes, since biometric data intrinsically involve genuine risks for the persons concerned if they are lost or used for purposes other than those for which they were intended".[8]

- Uanset at et privat, centralt register forudsættes at være i overensstemmelse med persondatalovens bestemmelser og Datatilsynets vilkår, rejser der sig en række spørgsmål i relation til datasikkerhed. Disse spørgsmål vedrører bl.a. hvem skal være dataansvarlig for registrets omfattende indsamling, registrering, behandling, sletning mv. af fortrolige personoplysninger. Vedligeholdelsen forudsætter en løbende opdatering af oplysninger, herunder gyldigheden af meddelte samtykker fra gæster, sletning af oplysninger ved tilbagekaldelse af samtykke samt den løbende ajourføring af oplysninger om karantæne vedrørende enkelte diskoteker/natklubber mv. Disse forhold er ikke afklaret i betænkningen, se s. 81.
- Det må forventes, at den personkreds, som skal kunne benytte registret, vil være relativt omfattende (dørmænd/bartendere m.fl.), hvis registret skal have en praktisk berettigelse. Dette fordrer en meget høj grad af datasikkerhed og intensiverer behovet for procedurer og kontrol med løbende vedligeholdelse og adgang til registret, herunder regler om logning.
- Organisationen Privacy International har påpeget[9], at der består en ikke ubetydelig fejlrate ved brugen af fingeraftryksteknologi, og at denne risiko ikke er erkendt i en bredere offentlighed. Dette rejser også spørgsmål i relation til fejlagtig accept eller afvisning af personer, se herved også artikel 29-gruppen, som har anført, at det er af uomgængelig nødvendighed, at sådanne systemer fejltestes – også vedrørende hensigtsmæssig personidentifikation – inden de bliver gennemført[10].
- Datatilsynet vil være tilsynsmyndighed på området. Et sådant tilsyn forudsætter væsentlige ressourcer henset til, at der er tale om et personfølsomme oplysninger på et relativt omfattende område. Dette forhold forstærkes af, at den dataansvarlige må antages at være en privat aktør, der ikke tidligere har skullet håndtere sådanne mængder af personfølsomme personoplysninger over et længere tidsrum.

c. Retssikkerhed

- Samtykke til brug for indsamling, registrering, sletning mv. af personoplysninger skal være udtrykt ved en frivillig, specifik og informeret viljestilkendegivelse, jf. persondatalovens § 3. Et samtykke kan tilbagekaldes efter persondatalovens § 38. Det er vigtigt, at gæsten grundigt informeres om konsekvenserne af en registrering samt retsvirkningerne af en tilbagekaldelse af et tidligere meddelt samtykke, herunder at årsagen til restaurationsforbuddet skal fjernes fra registret.
- Samtykke vil ofte blive givet under omstændigheder, som kan rejse spørgsmål i relation til, om dette er reelt. Det vil typisk blive givet ved besøg i nattelivet, hvor den person, som afgiver samtykket, ikke nærmere reflekterer over de konsekvenser et afgivet samtykke har i relation til omfanget af registrering.
- Restaurationsforbud kan meddeles allerede ved en sigtelse for et strafbart forhold. Såfremt sigtelsen frafaldes eller der senere sker frifindelse, kan det overvejes, om der skal gives en form for compensation ved fejl. Samme forhold kan gøre sig gældende i forbindelse med en meddelt karantæne.

3. Ligebehandlingsmæssige konsekvenser.

Det er Instituttets opfattelse, at oprettelsen af et centralt, privat register ikke rejser særlige ligebehandlingsmæssige problemer, idet ordningen forudsættes administreret ens over for alle restaurationsgæster. Det kan således ikke udelukkes, at et register endog kan have en vis positiv effekt i relation til at mindske usaglig forskelsbehandling.

Der henvises til j.nr. 2009-945-1435.

Med venlig hilsen

Jonas Christoffersen
Direktør