JUSTITSMINISTERIET

Folketinget
Retsudvalget
Christiansborg
1240 København K
DK Danmark

Dato: 7. april 2020
Kontor: HR-kontoret
Sagsbeh: Freia Kirkeskov-Hansen
Sagsnr.: 2020-0030-3934
Dok.: 1429781

Hermed sendes besvarelse af spørgsmål nr. 1071 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 13. marts 2020. Spørgsmålet er stillet efter ønske fra Rosa Lund (EL).

Nick Hækkerup

/

Michelle Argir Simonsen

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 1071 (Alm. del) fra Folketingets Retsudvalg:

> ”Giver et antal polititjenestemænds ikke sagligt begrundede brug af muligheder for indsigt i en kendt sportsudøvers konkrete politisag anledning til overvejelser om begrænsninger i adgangen til personfølsomme oplysninger i politiets it-systemer eller til andre forholdsregler, idet der henvises til artiklen ”Politifolk kaldt til alvorssnak: Snagede i Nicklas Bendtners voldssag” fra dr.dk den 6. marts 2020?”

Svar:

Justitsministeriet har til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra Rigspolitiet, der har oplyst følgende:

> ”*Tilsyn med medarbejdernes brug af politiets it-systemer*
> Rigspolitiet kan indledningsvis oplyse, at Rigspolitiet i overensstemmelse med reglerne i lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger (retshåndhævelsesloven), bekendtgørelse nr. 1078 af 20. september 2017 om politiets behandling af oplysninger i forbindelse med tværgående informationsanalyser og Rigspolitiets interne retningslinjer om informationssikkerhed fører legalitetsmæssig kontrol med medarbejderes anvendelse af politiets it-systemer. Dette sker navnlig gennem kontrol af logoplysninger. Logoplysninger er maskinelle registreringer af brugeraktiviteter i et it-system (eksempelvis indsamling, ændring, søgning eller sletning af oplysninger). Det bemærkes, at Rigspolitiet løbende er opmærksom på at sikre en forbedret it-understøttelse af Rigspolitiets muligheder for at understøtte denne kontrol.
>
> Hvis Rigspolitiet i forbindelse med en kontrol af logoplysninger identificerer en brugeradfærd, der umiddelbart ikke forekommer relevant for den pågældende medarbejders arbejdsopgaver, eller i øvrigt giver anledning til nærmere undersøgelser, udarbejder Rigspolitiet en rapport, der sendes til pågældendes tjenestested.
>
> Den endelige vurdering af, om en given brugeradfærd er berettiget, foretages af medarbejderens tjenestested – f.eks. den relevante politikreds – da det navnlig er tjenestestedet, der har den nødvendige indsigt i, hvilke opgaver den enkelte medarbejder varetager og dermed også indsigt i, hvorvidt en given brugeradfærd er berettiget eller ej.
>
> *Mulighed for at begrænse adgangen til personoplysninger*
> Rigspolitiet kan oplyse, at politiets ansatte i overensstemmelse med reglerne i retshåndhævelsesloven og Rigspolitiets interne retningslinjer om informationssikkerhed ikke må tildeles ad-

gang til og anvende it-systemer, som de ikke har et arbejdsbetinget behov for.

Rigspolitiet har herudover løbende fokus på, at adgangen til politiets it-systemer skal søges begrænset mest muligt, herunder i forbindelse med anskaffelse mv. af nye it-løsninger.

Flere af politiets centrale it-systemer er dog kendetegnet ved, at en relativ bred gruppe af medarbejdere har et arbejdsbetinget behov for at anvende dem i forbindelse med deres daglige opgavevaretagelse. Politiets sagsstyringssystem POLSAS og flere af politiets centrale systemer anvendes eksempelvis både i sager inden for strafferetsplejen og til at træffe afgørelse i administrative sager om udstedelse af tilladelser og bevillinger.

Politiets opgaveløsning forudsætter derudover et tæt samarbejde på tværs af afdelinger og politikredse, hvorfor medarbejderne også har et arbejdsbetinget behov for at kunne tilgå sager og oplysninger på tværs af organisationen, eksempelvis med henblik på at bringe kredsoverskridende kriminalitet til ophør. Det er derfor vigtigt, at efterforskere har mulighed for at søge i alle sager også på tværs af politikredse. Hvis en gruppe sager bliver lukket af hensyn til risikoen for, at medarbejdere uberettiget vil slå dem op, vil dette også afskære efterforskere fra at slå sagerne op, hvis det på et senere tidspunkt bliver relevant. Det kan f.eks. være, hvis der er tale om gentagelse af en forbrydelse, eller hvis forskellige forbrydelser skal kunne kobles sammen. Derfor er begrænsning i adgangen til sager i POLSAS ikke hensigtsmæssig, idet det ikke på forhånd er muligt at vide, hvem der skal kunne tilgå sagen fremadrettet.

Bl.a. på denne baggrund – og foruden arbejdet med kontrol af logoplysninger som er beskrevet ovenfor – har Rigspolitiet løbende fokus på at uddanne medarbejdere i, hvornår og hvordan de må anvende politiets it-systemer. Eksempelvis lancerede Rigspolitiet og Rigsadvokaten i efteråret 2018 en kampagne om god adfærd i politi og anklagemyndighed, der bl.a. fokuserede på, hvornår registeropslag er uberettigede.

Rigspolitiet har således løbende fokus på at sikre, at politiets medarbejdere er bekendt med rammerne for den adgang til politiets systemer mv, som de tildeles som led i deres ansættelse og på at sikre en løbende overvågning af, hvordan personoplysninger, som politiet behandler, bliver tilgået og anvendt af medarbejderne.

Personalemæssige tiltag
Rigspolitiet kan oplyse, at Rigspolitiet også ud over den konkrete sag, generelt har iværksat en række tiltag for at hindre bl.a. registermisbrug i politiet, og at der løbende pågår planlægning af nye tiltag.

Rigspolitiet kan i den forbindelse oplyse, at der er iværksat et større initiativ om informationssikkerhedsadfærd. Dette initiativ har registeropslag som et klart og vedvarende fokusområde, og initiativet har bl.a. til formål at højne medarbejdernes forståelse for det ansvar, der er forbundet med at have adgang til politiets systemer og registre, herunder hvornår der er tale om et uberettiget opslag. Som eksempel på et initiativ kan nævnes, at hver politikreds og Rigspolitiet har udpeget to databeskyttelsesambassadører, som konkret og løbende skal informere og vejlede medarbejderne omkring reglerne for anvendelse politiets registre og medarbejdernes tavshedspligt.

Rigspolitiet kan herudover oplyse, at der løbende udvikles materiale om informationssikkerhed, som skal gøre det lettere for alle politikredsene og Rigspolitiets områder at arbejde for, at alle medarbejdere får grundig indsigt i informationssikkerhed.

Informationssikkerhed er ligeledes et fokusområde, når Rigspolitiet ansætter nye medarbejdere, og alle nye medarbejdere skal i forbindelse med introforløbet gennemføre et kursus via e-learning omkring informationssikkerhed. Derudover indskærpes reglerne for anvendelse af politiets registre på introduktionsdagene.

Ansættelsesretlige konsekvenser
Hvis en medarbejder foretager et uberettiget registeropslag eller på anden vis uberettiget gør sig bekendt med oplysninger, eller hvis medarbejderen deler oplysninger med andre, uden at det er tjenstligt begrundet, vil det endvidere kunne få ansættelsesretlige konsekvenser. Det vil i de alvorligste tilfælde udgøre en overtrædelse af straffeloven, hvilket medarbejderne i politiet er informerede om. I den forbindelse skal det bemærkes, at sanktionsniveauet for overtrædelse af reglerne på området løbende vurderes i forhold til, om niveauet er proportionelt i forhold til forholdets karakter og grovhed."