JUSTITSMINISTERIET

Folketinget
Retsudvalget
Christiansborg
1240 København K
DK Danmark

Dato: 18. december 2019
Kontor: Databeskyttelseskontoret
Sagsbeh: Mikkel Reenberg
Sagsnr.: 2019-0030-3244
Dok.: 1328436

Hermed sendes besvarelse af spørgsmål nr. 453 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 4. december 2019. Spørgsmålet er stillet efter ønske fra Karina Lorentzen Dehnhardt (SF).

Nick Hækkerup

/

Anders Lotterup

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 453 (Alm. del) fra Folketingets Retsudvalg:

> ”Vil ministeren udlægge, hvordan lovgivningen imødegår denne type overvågning samt hvor mange sager, politiet har haft af den karakter, idet ministeren også bør tage stilling til om et dansk forbud mod stalker-apps kan lade sig gøre og eventuelle fordele og ulemper i den forbindelse, jf. artiklen ””Det er virkelig noget, der griber om sig.” Smartphones er blevet stalkeres smarteste våben” fra Zetland.dk den 3. december 2019?”

Svar:

1. Danskerne skal kunne færdes frit, uden at de igennem applikationer på deres smartphone imod deres vilje bliver overvåget. Den overvågning, som beskrives i den omtalte artikel, er helt uacceptabel.

Det følger af straffelovens § 264 b, at det er strafbart uberettiget at registrere en andens færden ved hjælp af gps eller et andet lignende apparat. En overtrædelse medfører bøde eller fængsel i indtil 6 måneder.

2. Straffelovens § 264 b blev indsat ved lov nr. 1719 af 27. december 2018 om ændring af straffeloven, retsplejeloven, erstatningsansvarsloven og medieansvarsloven (Freds- og ærekrænkelser m.v.). Det fremgår af forarbejderne til bestemmelsen, jf. lovforslag nr. L 20 af 8. oktober 2018, at gerningsindholdet består i selve registreringen i form af indsamling eller lagring af data ved hjælp af en gps eller et andet lignende apparat, med henblik på at gerningsmanden gennem de registrerede oplysninger vil kunne følge en anden (bestemt) persons færden, jf. pkt. 2.5.2 i lovforslagets almindelige bemærkninger.

Bestemmelsen finder anvendelse, hvis der er anvendt en gps eller andet lignende teknisk udstyr til at registrere en andens færden. Der kan f.eks. være tale om en gps, der er anbragt i eller på en persons bil, taske eller tøj. Det er ikke afgørende, om gerningsmanden kan følge personens færden ved hjælp af signaler, der løbende sendes fra gps’en, eller om gps’en lagrer koordinater, som gerningsmanden efterfølgende skaffer sig adgang til. Bestemmelsen omfatter også overvågning ved hjælp andre lignende apparater, f.eks. ved pejling af radiosignaler, der udsendes af noget, som personen har med sig, herunder en mobiltelefon, tablet mv., eller ved hjælp af et videokamera, der viser en anden persons færden. Det afgørende er, at gerningsmanden re-

gistrerer en anden (bestemt) persons færden og dermed kan følge dennes færden uden selv at være til stede.

Det er en betingelse, at gerningsmanden har forsæt til at foretage registreringen, hvilket typisk vil komme til udtryk ved, at gerningsmanden selv har anbragt det anvendte apparat. Gerningsindholdet er fuldbyrdet, når registreringen er foretaget, hvis registreringen er egnet til at følge den anden persons færden.

Det fremgår endvidere af forarbejderne, at f.eks. forældres overvågning ved hjælp af gps eller andet lignende apparat af mindreårige, hjemmeboende børn i almindelighed ikke vil skulle anses for uberettiget overvågning efter § 264 b. Derimod vil overvågning ved hjælp af gps af en kæreste, partner, ægtefælle mv. i almindelighed skulle anses for uberettiget overvågning efter § 264 b, jf. pkt. 2.5.3 i lovforslagets almindelige bemærkninger.

Tilfælde, hvor gerningsmanden selv har slået en indbygget gps i forurettedes smartphone til, så telefonen lagrer oplysninger om den pågældendes færden, som gerningsmanden senere skaffer sig adgang til, vil efter omstændighederne skulle straffes efter både §§ 264 b og 263, stk. 1, jf. lovforslag nr. L 20 af 30. oktober 2018, de specielle bemærkninger til § 1, nr. 8.

Efter straffelovens § 263, stk. 1, straffes med bøde eller fængsel indtil 1 år og 6 måneder den, der uberettiget skaffer sig adgang til en andens datasystem eller data, som er bestemt til at bruges i et datasystem. Det fremgår af forarbejderne til bestemmelsen, at der ved datasystem forstås computere og andet elektronisk udstyr, hvis udstyret har samme funktioner svarende til dem, der findes i computere, f.eks. smartphones og tablets, jf. samme lovforslag, de specielle bemærkninger til § 1, nr. 4. Bestemmelsen omfatter meget forskelligartede forhold, herunder at en gerningsmand skaffer sig adgang til en andens computer eller smartphone.

3. Justitsministeriet har til brug for besvarelsen desuden indhentet en udtalelse fra Rigspolitiet, der har oplyst følgende:

> ”Rigspolitiet kan indledningsvis oplyse, at det fremgår af politiets sagsstyringssystem (POLSAS), at der i perioden fra den 1. januar 2019 til den 1. december 2019 er registeret 730 anmeldelser om overtrædelse af straffelovens § 263, stk. 1 (uberettiget adgang til andens datasystem eller data, som er bestemt til at bruges i et datasystem), og at der i perioden fra den 1. januar 2019 til den 1. december 2019 er registreret ni anmeldelser om

overtrædelse om straffelovens § 264 b (uberettiget registrering af en andens færden).

De anmeldte sager vedrørende overtrædelse af straffelovens § 263, stk. 1, dækker over en række forskellige forhold, herunder at skaffe sig adgang til andres mail eller digitale postkasse via misbrug af nem-id, installation af overvågningsapplikationer mv. Det er imidlertid ikke muligt uden foretagelse af en manuel gennemgang af de enkelte sager at opgøre, hvor mange af disse sager, der specifikt vedrører digital stalking.

De anmeldte sager vedrørende overtrædelse af straffelovens § 264 b omhandler fund af GPS-sporingsenhed i en rygsæk (én sag) og fund af GPS-sporingsenheder fundet på køretøjer (otte sager). De sidstnævnte sager har alle stalkinglignende karakter.

Det er Rigspolitiets vurdering, at den stigende digitalisering i samfundet og de mange nye applikationer mv. øger risikoen for overvågning af eksempelvis en partner eller tidligere partner.

Som nævnt i artiklen er det allerede ulovligt at overvåge personer ved anvendelse af GPS eller lignende, ligesom det er ulovligt uberettiget at skaffe sig adgang til datasystemer, gøre sig bekendt med indholdet af et brev eller anden lukket meddelelse samt hemmeligt af aflytte telefonsamtaler eller samtaler i et lukket møde. En række applikationer giver mulighed for at indhente denne type data via eksempelvis en telefon, hvilket som nævnt er ulovligt, hvis det sker uden samtykke. Nogle af disse applikationer fremstår dog med et legalt formål som for eksempel muligheden for at overvåge egne børns færden. Det er altså tale om en form for dual-use anvendelse af disse applikationer, hvilket vil sige, at der både er en lovlig og en ulovlig anvendelsesmulighed. Dette betyder, at der ikke kan straffes for besiddelse af disse applikationer, medmindre det kan bevises, at de anvendes på lovstridig vis.

Ved indførelsen af et forbud mod besiddelse af denne type applikationer, kan det vise sig vanskeligt at afgrænse uønskede applikationer fra de ønskede. Endvidere kan et forbud ramme personer, som anvender disse applikationer til et legitimt formål, ligesom det i nogen grad vil være muligt at stalke personer ved anvendelse af onlineværktøjer, som således ikke vil være omfattet af et forbud mod brugen af visse applikationer.

Såfremt man forbyder distribution af denne type applikationer, vil det sandsynligvis være muligt, at få Apple og Google og tilsvarende store virksomheder til at blokere for danskernes adgang til disse applikationer. Så længe de pågældende applikationer er lovlige i andre lande, vil det dog fortsat være muligt at hente sådanne applikationer ved anvendelse af VPN-forbindelser eller via udbydere, der ikke er rettet mod et dansk marked,

> og derfor ikke forholder sig til dansk lovgivning. Endvidere vil det være muligt at hente denne type applikationer via de mere uregulerede områder på internettet, herunder darkweb.
>
> Et forbud mod besiddelse eller distribution af de pågældende applikationer vil således kræve nærmere overvejelser/undersøgelser.
>
> Rigspolitiet skal afslutningsvis oplyse, at Rigspolitiet i 2018 udsendte retningslinjer til politikredsene om forebyggelse af digital stalking, som kan anvendes i forbindelse med behandling af sager om chikane, forfølgelse og stalking. Vejledningen er endvidere fremsendt til en række eksterne aktører på området."

I lyset af oplysningerne fra Rigspolitiet, herunder at et forbud vil være relativt nemt at omgå, og at applikationerne også kan bruges til saglige formål, og fordi en uberettiget overvågning som nævnt vil være strafbar, er det ikke min opfattelse, at bestemte applikationer bør forbydes.

4. Justitsministeriet har til brug for besvarelsen endvidere indhentet en udtalelse fra Datatilsynet, der har oplyst følgende:

> "Datatilsynet har alene vurderet de databeskyttelsesretlige implikationer, der kan relateres til det rejste spørgsmål. De situationer hvor overvågningen sker, ved indgreb i eller uautoriseret adgang til de enheder der benyttes, forudsættes behandlet efter straffelovens regler herom.
>
> Datatilsynet bemærker dog, at den, der måtte overvåge på den beskrevne måde, aldrig vil have den fornødne hjemmel til at behandle oplysningerne i databeskyttelsesforordningens og databeskyttelseslovens forstand.
>
> Generelt har Datatilsynet, på tilsynets hjemmeside, givet rådgivning om og vejleding i, hvordan en person som bruger kan få overblik over de digitale aftryk, personen sætter ved brug af forskellige applikationer. Senest har tilsynet i tre små videoer, beskrevet hvordan en person som bruger kan mindske eller fjerne sådanne digitale aftryk.
>
> En udbyder af applikationer skal efter databeskyttelsesforordningens bestemmelser påse, at applikationen har en passende sikkerhed, jf. navnlig databeskyttelsesforordningens artikel 32.
>
> Det vil i forhold til de situationer, der beskrives i spørgsmålet betyde, at oplysninger fra applikationen, som brugeren ikke ønsker at dele, ikke kan tilgås af uvedkommende, eller spredes på en måde, der ligger uden for brugerens kontrol.

Princippet om databeskyttelse gennem design og standardindstillinger i databeskyttelsesforordningens artikel 25 indebærer samtidig, at brugernes rettigheder skal tilgodeses gennem måden applikationen er lavet og virker på. Indstillingerne skal blandt andet sikre, at personoplysninger ikke uden brugerens egen medvirken eksponeres for en bredere kreds.

Medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde eller fængsel indtil 6 måneder den, der overtræder bl.a. den dataansvarliges og databehandlerens forpligtelser i henhold til databeskyttelsesforordningens artikel 8, 11, 25-39, 42 eller 43, jf. databeskyttelseslovens § 41, stk. 1, nr. 1."