



JUSTITSMINISTERIET

Dato: 30. marts 2020
Kontor: Strafferetskontoret
Sagsbeh: Iren Mirmojtahedi
Sagsnr.: 2020-0090-1964
Dok.: 1443304

Ændringsforslag
til
Forslag til lov om ændring af straffeloven
(Skærpet straf for lovovertrædelser med baggrund i eller sammenhæng
med covid-19) (L 157)

Æ n d r i n g s f o r s l a g

Af *justitsministeren*, tiltrådt af: ...

Til titlen

1) Efter »**straffeloven**« indsættes: »**og retsplejeloven**«.

[Udvidelse af lovens område]

2) I *undertitlen* indsættes efter »covid-19«: »og blokering af hjemmesider, hvorfra der begås visse lovovertrædelser, som har baggrund i eller sammenhæng med covid-19«

[Ændret undertitel som følge af forslaget om blokering af hjemmesider]

Ny paragraf

3) Efter § 1 indsættes som ny paragraf:

»§ 01

I retsplejeloven, jf. lovbekendtgørelse nr. 938 af 10. september 2019, foretages følgende ændringer:

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

1. I § 791 d, stk. 1, indsættes som 2. pkt.:

»Blokering kan endvidere ske, hvis der er grund til at antage, at der fra hjemmesiden begås en overtrædelse af straffelovens § 161, § 163, § 171, § 189, § 263 a, § 276, §§ 278-283, §§ 289-290 a, § 300 a, § 301 eller § 303, som har baggrund i eller sammenhæng med covid-19-epidemien i Danmark.«

[Udvidet mulighed for blokering af hjemmesider]

2. I § 791 d indsættes som stk. 6:

»Stk. 6. Såfremt indgrebets øjemed i medfør af stk. 1, 2. pkt., ville forspildes, hvis retskendelse skulle afventes, kan politiet træffe beslutning om blokering. I så fald skal politiet snarest muligt og senest inden 24 timer fra indgrebets iværksættelse forelægge sagen for retten. Retten afgør ved kendelse, om indgrebet kan godkendes, og om det kan opretholdes. Burde indgrebet efter rettens opfattelse ikke have været foretaget, skal retten give meddelelse herom til Justitsministeriet.«

[Mulighed for at foretage blokering på øjemedet]

Til § 2

4) I stk. 3 indsættes efter »§ 1, nr. 1,«: » retsplejelovens § 791 d, stk. 1, 2. pkt., som affattet ved denne lovs § 01, nr. 1, og retsplejelovens § 791 d, stk. 6, som affattet ved denne lovs § 01, nr. 2,«.

[Udvidelse af solnedgangsklausulen]

B e m æ r k n i n g e r

Til nr. 1

Ændringen er en følge af ændringsforslag nr. 3, hvorefter lovens område udvides til også at omfatte ændringer i retsplejeloven.

Til nr. 2

Ændringen er en følge af ændringsforslag nr. 3, der indebærer, at der indføres mulighed for blokering af hjemmesider, hvorfra der begås lovovertrædelser, som har baggrund i eller sammenhæng med covid-19-epidemien i Danmark.

Til nr. 3

Med lovforslagets § 1, nr. 1, foreslås det at indsætte en ny bestemmelse i straffelovens § 81 d, hvorefter den straf, der er foreskrevet i en række bestemmelser i straffeloven kan forhøjes indtil det dobbelte, hvis lovovertrædelsen har baggrund i eller sammenhæng med covid-19-epidemien i Danmark. Straffen kan endvidere forhøjes således, at den bliver fire gange så høj, hvis lovovertrædelsen har fundet sted under sådanne omstændigheder, at der uberettiget er opnået eller søgt opnået lån, kredit, støtte, tilskud eller lignende kompensation fra hjælpepakker til imødegåelse af skadevirkninger ved covid-19-epidemien.

Formålet med lovforslaget er at sætte ind over for lovovertrædelser, der har baggrund i eller sammenhæng med covid-19-epidemien i Danmark. Det gælder bl.a. kriminalitetsformer, hvor borgerens tillid til offentlige myndigheder i en krisesituation som den foreliggende udnyttes.

For at sætte yderligere ind og sikre en effektiv bekæmpelse af covid-19-relateret it-kriminalitet foreslås det med dette ændringsforslag at udvide anvendelsesområdet for retsplejelovens § 791 d.

Center for Cybersikkerhed (CFCS) har konstateret et antal hjemmesider, der via phishing forsøger at udnytte covid-19-situationen. CFCS har således konstateret, at der er oprettet en række domænenavne, hvor navnet ligger tæt op ad forskellige myndigheders officielle domænenavne, herunder på sundhedsområdet. Det er konstateret, at visse af disse domænenavne, der udgiver sig for at være Sundhedsstyrelsen, anvendes til at franarre borgere personlige oplysninger i form af NemID-nøglekort.

Rigspolitiet har i tilknytning hertil konstateret en tendens til oprettelse af domænenavne indeholdende ord som ”coronavirus”, ”coronasmitte”, ”covid-19” samt lignende synonymmer. Der er pr. 23. marts 2020 afdækket 255 domæner, der vurderes at have tilknytning til covid-19. Rigspolitiet vurderer, at mange nye websites enten er opsat med henblik på indtjening via reklamemidler eller med kriminelle hensigter. Rigspolitiet har pr. 23. marts 2020 fundet 20 domæner, der vurderes at være mistænkelige. Det vurderes, at der enten er tale om falske webshops eller falske myndighedshjemmesider.

For så vidt angår de falske webshops har Rigspolitiet oplyst, at der er tale om forretninger som foregiver at sælge håndsprit, mundbind og engangshandsker mv.

Herudover har Rigspolitiet oplyst, at de falske myndighedshjemmesider anvendes til nye såkaldte phishing-kampagner, der bl.a. har til formål at frarøve privatpersoner deres kreditkortoplysninger, som derefter misbruges. I nogle tilfælde er det gerningsmændene selv, der benytter oplysningerne, i andre tilfælde sælges oplysningerne videre til andre kriminelle. Phishing kan – afhængig af den konkrete fremgangsmåde og brugen af oplysningerne – være strafbart efter reglerne om bedrageri eller databedrageri, jf. straffelovens §§ 279 og 279 a.

Det følger af den gældende bestemmelse i retsplejelovens § 791 d, stk. 1, at der kan ske blokering af en hjemmeside, hvis der er grund til at antage, at der fra hjemmesiden begås en overtrædelse af straffelovens §§ 114-114 i, 119 eller 119 a.

Ved blokering forstås en ordning, der er rettet mod danske internetudbydere med henblik på direkte DNS-blokering fra udbyderens side af hjemmesiden med ulovligt materiale. DNS-blokering medfører, at forsøg på at opnå adgang til siden automatisk afvises af internetudbyderen. Bestemmelsen forudsætter, at afvisningen vil være ledsaget af en tekst, hvoraf det fremgår, at politiet har opnået rettens kendelse til at blokere den pågældende hjemmeside, og at eventuelle indsigelser kan rettes til politiet.

Kravet om, at der skal være »grund til at antage« skal forstås i overensstemmelse med det tilsvarende udtryk i retsplejelovens §§ 803 og 804 om beslaglæggelse over for ikke-mistænkte og edition.

Kravet om, at der fra hjemmesiden begås en overtrædelse af straffelovens §§ 114-114 i, 119 eller 119 a, indebærer, at siden skal indeholde tekst, video eller lyd mv., der udgør en sådan overtrædelse.

Det foreslås at indsætte et *stk. 1, 2. pkt.*, hvorefter blokering kan ske, hvis der er grund til at antage, at der fra hjemmesiden begås en overtrædelse af straffelovens § 161, § 163, § 171, § 189, § 263 a, § 276, §§ 278-283, §§ 289-290 a, § 300 a, § 301 eller § 303, som har baggrund i eller sammenhæng med covid-19-epidemien i Danmark.

Forslaget indebærer, at der på samme måde som for hjemmesider, hvorfra der begås overtrædelser af straffelovens §§ 114-114 i, 119 eller 119 a, fremover vil kunne ske blokering, når der er tale om en overtrædelse af straffelovens § 161, § 163, § 171, § 189, § 263 a, § 276, §§ 278-283, §§ 289-290 a, § 300 a, § 301 eller § 303, som har baggrund i eller sammenhæng med covid-19-epidemien i Danmark.

Vurderingen af, om der er »grund til at antage«, at der fra hjemmesiden begås en af de pågældende lovovertrædelser, skal foretages ud fra sagens samlede omstændigheder, herunder fremtoningen af domænenavnet og hjemmesiden. Det kan i den forbindelse bl.a. indgå, om domænenavnet eller hjemmesidens titel har stor lighed med en hjemmeside for en myndighed, organisation, koncessioneret virksomhed eller lignende, og om besøgende på hjemmesiden opfordres til at indtaste NEM-id oplysninger, cpr-nummer og/eller kreditkortoplysninger. Andre oplysninger på hjemmesiden kan ligeledes indgå i vurderingen, herunder forkert/falsk cvr-nummer og kontaktoplysninger, der henviser til uregistrerede taletidskort, forkerte/falske adresser mv. Det kan ligeledes indgå, om besøgende opfordres til at rette henvendelse via f.eks. e-mail eller telefon til kontaktoplysninger, der er falske eller har stor lighed med en dansk myndigheds kontaktoplysninger.

Registreringen af et domænenavn vil ikke i sig selv give grund til at antage, at der begås en af de pågældende lovovertrædelser med baggrund i eller sammenhæng med covid-19-epidemien i Danmark, idet registreringen ikke nødvendigvis vil være strafbar. Det forudsættes, at hjemmesiden har et indhold i form af lyd, tekst, video, links, tekniske indretninger eller lignende, der udgør en overtrædelse af de pågældende bestemmelser. Domænenavnet vil dog, som nævnt ovenfor, indgå som et moment i den samlede vurdering.

Kravet om, at der fra hjemmesiden »begås« en overtrædelse af de pågældende bestemmelser indebærer, at hjemmesiden på blokeringstidspunktet skal have et indhold, der udgør en overtrædelse. Blokering vil dermed ikke kunne ske med henvisning til, at tidligere indhold på hjemmesiden, som nu er fjernet, udgjorde en overtrædelse af straffelovens § 161, § 163, § 171, § 189, § 263 a, § 276, §§ 278-283, §§ 289-290 a, § 300 a, § 301 eller § 303.

For så vidt angår betingelsen om, at den pågældende lovovertrædelse har »baggrund i eller sammenhæng med covid-19-epidemien i Danmark« henvises til bemærkningerne til lovforslagets § 1, nr. 1.

Det er også muligt for politiet at beslaglægge hjemmesider efter reglerne i retsplejelovens kapitel 74. Beslaglæggelse af hjemmesider anvendes hovedsageligt af politiet i de tilfælde, hvor hjemmesiden administreres i Danmark. Det vil i praksis være hjemmesider, der ender på ".dk", som er administreret af organisationen DK Hostmaster.

Når en hjemmeside er beslaglagt, kan den ikke længere tilgås af besøgende på internettet, der i stedet typisk i en periode vil blive mødt med en besked om, at rettighederne til hjemmesiden er overført til politiet eller anklagemyndigheden.

I det omfang, der er tale om en hjemmeside, som administreres i udlandet, kan det i praksis være vanskeligt at gennemføre en beslaglæggelse, idet beslaglæggelsen forudsætter bistand fra det land, hvor hjemmesiden administreres. Det er muligt at anmode andre lande om retshjælp til gennemførelsen af en beslaglæggelse af en udenlandsk hjemmeside, men det er ofte meget tidskrævende, ligesom der er lande, der ikke yder denne form for retshjælp, jf. tillige bemærkningerne til forslag til lov om ændring af retsplejeloven og forskellige andre love (Blokering af hjemmesider og stop af offentlige ydelser til fremmedkrigere), jf. Folketingstidende 2016-17, A, L 192, som fremsat, side 12.

Rigspolitiet har oplyst, at de anmeldelser, som politiet har modtaget vedrørende covid-19-relaterede phishing-kampagner, primært ses at vedrøre udenlandske domæner, herunder ".net", ".com" og ".eu". På disse hjemmesider bliver den besøgende eksempelvis bedt om at indtaste NEM-id oplysninger og kan efterfølgende konstatere, at der er foretaget uberettigede hævnninger på den pågældendes bankkonto, optagelse af lån i den pågældendes navn mv. De falske webshops, som Rigspolitiet har kendskab til, er derimod primært oprettet med det danske domænenavn ".dk".

Tilsvarende har CFCS oplyst, at de domænenavne, der er oprettet med enslydende navne til forskellige danske myndigheder primært administreres i udlandet, hvorfor det kan være vanskeligt at anvende beslaglæggelsesreglerne.

Ligesom for den gældende § 791 d, forudsættes retsplejelovens regler om beslaglæggelse dog fortsat anvendt, når denne fremgangsmåde vurderes praktisk anvendelig.

Den gældende bestemmelse i retsplejelovens § 791 d indeholder ikke en *periculum in mora*-regel. En sådan regel indebærer, at politiet kan udføre et tvangsindgreb på øjemedet og efterfølgende indbringe spørgsmålet for retten. Retten vil herefter prøve, om betingelserne for tvangsindgrebet er opfyldt, og om der var tale om en situation, hvor indgrebets øjemed ville være forspildt, hvis rettens kendelse skulle afventes.

Det foreslås at indsætte et nyt *stk. 6*, der giver politiet hjemmel til at træffe beslutning om blokering i de tilfælde, hvor indgrebets øjemed i medfør af *stk. 1, 2. pkt.*, ville forspildes, hvis retskendelse skulle afventes. Det foreslås endvidere, at politiet snarest muligt og senest inden 24 timer fra indgrebets iværksættelse skal forelægge sagen for retten. Retten afgør ved kendelse, om indgrebet kan godkendes, og om det kan opretholdes. Burde indgrebet efter rettens opfattelse ikke have været foretaget, skal retten give meddelelse herom til Justitsministeriet.

Forslaget indebærer, at politiet vil kunne iværksætte indgrebet ud fra en øjemedsbetragtning, når blokeringen sker efter den foreslåede § 791 d, *stk. 1, 2. pkt.*

Den foreslåede bestemmelse skal ses i lyset af, at phishing-angreb i helt særlig grad er tidskritiske. Der kan således på få minutter og med få omkostninger udsendes store mængder af e-mails eller sms-beskeder som led i en phishing-kampagne. Hvis det skal sikres, at det domænenavn, som phishing-kampagnen linker til, bliver blokeret, inden et stort antal personer har reageret på kampagnen, vil det i nogle tilfælde være nødvendigt, at politiet kan iværksætte blokeringen hurtigt og derefter indbringe spørgsmålet for retten inden 24 timer.

Det er endvidere vurderingen, at hensynet til at kunne gribe hurtig ind over for bl.a. misinformation og misbrug under den aktuelle covid-19-epidemi gør sig gældende i en sådan helt særlig grad, at der er behov for at indføre en ordning med mulighed for blokering på øjemedet.

Til nr. 4

Under hensyntagen til lovforslagets formål og kontekst bør en udvidelse af anvendelsesområdet for blokering af hjemmesider ligeledes begrænses tidsmæssigt. Det foreslås derfor, at ændringsforslag nr. 3 om udvidelse af anvendelsesområdet for blokering af hjemmesider bliver omfattet af lovforslagets såkaldte ”solnedgangsklausul”, hvorefter loven automatisk ophæves

den 1. marts 2021, medmindre Folketinget forinden beslutter at forlænge lovens gyldighedsperiode.

Hvis solnedgangsklausulen træder i kraft, uden at Folketinget forinden beslutter at forlænge lovens gyldighedsperioden, vil retsgrundlaget for de eventuelt iværksatte blokeringer ikke længere være til stede. Det forudsættes derfor, at blokeringer iværksat efter lovens § 01, nr. 1, og nr. 2, fjernes senest samtidig med ophævelse i medfør af den foreslåede § 2, stk. 3.

Det forudsættes således, at politiet efter en eventuel ophævelse af bestemmelserne retter henvendelse til udbydere med henblik på at få blokeringen fjernet.

Som det fremgår af bemærkninger til ændringsforslag nr. 3 og bemærkningerne til forslag til lov om ændring af retsplejeloven og forskellige andre love (Blokering af hjemmesider og stop af offentlige ydelser til fremmedkrigere), jf. Folketingstidende 2016-17, A, L 192, som fremsat, side 12, forudsættes retsplejelovens regler om beslaglæggelse anvendt, når denne fremgangsmåde vurderes praktisk anvendelig.

Ophævelse af den foreslåede bestemmelse i retsplejelovens § 791 d, stk. 1, 2. pkt., har ikke indflydelse på de gældende regler om beslaglæggelse. Beslaglæggelsen af hjemmesider vil således – også efter en ophævelse af § 791 d, stk. 1, 2. pkt. – kunne opretholdes efter de gældende regler.