TfK2018.814

Retspleje 11.414.533.535.635.735.9

Politiets hjemmel til »hacking« som led i en efterforskning

♦ *Retsplejeloven indeholder ingen udtrykkelig bestemmelse om, hvornår politiet kan skaffe sig hemmelig adgang til private hjemmesider mv. på internettet. I stedet reguleres politiets »hacking« efter reglerne om ransagning, dataaflæsning og indgreb i meddelelseshemmeligheden. Højesteret har i U 2012.2614 H fastslået, at politiets hemmelige adgang med rette kode til en mistænkts Facebook- og Messenger-profiler skulle afgøres som gentagen, hemmelig ransagning. I artiklen diskuteres rækkevidden af Højesterets kendelse, herunder om reglerne om hemmelig ransagning nu må antages at udgøre den almindelige hjemmel for politiets »hacking«. Desuden behandles de retlige aspekter ved den situation, hvor politiet ved undersøgelse af beslaglagte computere og mobiltelefoner får adgang til digitale brugerkonti mv., som kan følges online fremadrettet, hvilket aktualiserer spørgsmålet, om der herved indledes en hemmelig ransagning, der skal opfylde retsplejelovens betingelser.*

Af ph.d.-stipendiat Lene Wacher Lentz, IECC, Juridisk Institut, Aalborg Universitet

1. Indledning

IT-kriminalitet i form af »hacking« er i stigning. En opgørelse fra Rigspolitiets Statistikenhed viser en støt stigning i antallet af anmeldelser om uberettiget adgang til it-systemer, jf. straffelovens § 263, stk. 2, i perioden fra 2008, hvor dansk Politi modtog 32 anmeldelser til 2017, hvor politiet modtog 418 anmeldelser.[1] Som mest spektakulære sager ses *CSC-sagen*, U 2015.3615 Ø, om uberettiget adgang til dansk politis registre, herunder kriminalregisteret, kørekortregisteret, CPR-registeret mv., og *Se og Hør-sagen*, U 2017.3544 Ø, hvor »tystys«-kilden skaffede sig uberettiget adgang til oplysninger om betalingstransaktioner, som han videresolgte til ugebladet Se og Hør.

Anmeldelser om uberettiget rådighedshindring efter straffelovens § 293, stk. 2, som bl.a. omfatter DDoS-angreb, hvor en server angribes af så mange forespørgsler, at systemet lukker helt eller delvist ned, er ligeledes stigende. I samme 10-årige periode ses en støt stigning i antallet, fra 3 anmeldelser i 2008 til 44 anmeldelser i 2017.[2]

Ifølge Europols »Internet Organised Crime Threat Assessment« (IOCTA) fra 2017, er især »ransomware«, hvor informationssystemer låses med krav om løsepenge, i stærk stigning. IOCTA-rapporten fremhæver WannaCry ransomware-angrebet fra den 12. maj 2017 som et skræmmende eksempel, hvor op mod 300.000 mål i over 150 lande blev ramt, inklusiv en række højt-profilerede mål såsom the UK's National Health Service, det spanske teleselskab Telefónica og logistikvirksomheden FedEx.[3]

Politiets metoder og tekniske formåen udvikles i disse år tilsvarende for at komme på omgangshøjde med den nye digitale kriminalitet, uden at de præcise metoder dog af forståelige årsager kommer til offentlighedens kendskab. Udover at denne form for efterforskning tilføres ressourcer og tekniske kompetencer, er det også vigtigt at sikre klare juridiske rammer for disse nye digitale efterforskningsmetoder, så der skabes retssikkerhed for de berørte borgere.

Formålet med denne artikel er at analysere, hvilken lovhjemmel der gælder, når politiet ønsker at gøre brug af metoden, »hacking«, hvor der skaffes hemmelig adgang til private data i et informationssystem. Et sådant indgreb er ikke udtrykkeligt reguleret i retsplejeloven, men reguleres i stedet af bestemmelserne om ransagning, dataaflæsning og indgreb i meddelelseshemmeligheden.

Centralt i analysen indgår U 2012.2614 H, hvor Højesteret tog stilling til en situation, hvor politiet med rette koder på egen hånd kunne skaffe sig adgang til en mistænkts profiler på Facebook og Messenger. Højesterets vurderede, at indgrebet skulle betragtes som en hemmelig ransagning. I det følgende vurderes rækkevidden af Højesterets kendelse, hvori indgår, om hemmelig ransagning nu må antages at udgøre politiets almindelige hjemmel til »hacking«, hvilket vil efterlade reglerne om dataaflæsning med et begrænset, praktisk anvendelsesområde. Spørgsmålet er, om politiet har en tilstrækkelig klar hjemmel til som led i en efterforskning at få hemmelig adgang til private datasystemer.

I forlængelse af denne hjemmels-problematik, behandler artiklen desuden i afsnit 5 den særlige situation, hvor politiet undersøger en beslaglagt computer eller mobiltelefon, hvor der samtidig i browservinduer åbnes profiler mv. hvilket giver politiet onlineadgang til at følge med i kommunikation mv. Spørgsmålet er, om hjemlen til en sådan fremadrettet efterforskning er indeholdt i beslaglæggelsen, eller om der i stedet iværksættes en hemmelig ransagning, som kræver, at retsplejelovens restriktive betingelser herfor er opfyldt.

2. Politiets »hacking« som tvangsindgreb mod borgeren

Politiet er i almindelighed berettiget til at gøre sig bekendt med offentligt tilgængelige data til brug for en efterforskning, hvilket nu udtrykkeligt fremgår af politilovens § 2 a, stk. 2.[4] Er der derimod tale om, at politiet i en efterforskning skaffer sig adgang til private, beskyttede data, vil dette være et indgreb i borgerens privatliv.

---

1 Rekvirerede tal fra Rigspolitiets Statistikenhed, opgørelse over anmeldelser og sigtelser pr. 13. marts 2018. Tallene viser ligeledes en stigning siden 2008 i anmeldelser om afpresning efter straffelovens § 281, dog uden at det er muligt at sondre mellem den traditionelle afpresning og den digitale variant »ransomware«.

2 Rekvirerede tal fra Rigspolitiets Statistikenhed pr. 13. marts 2018.

3 Iocta-rapporten s. 19. Tilgængelig på Europols hjemmeside, www.europol.europa.eu.

4 Lov nr. 671 af 8. juni 2017, trådt i kraft den 22. september 2017 ved bekendtgørelse nr. 1076 af 20. september 2017. For politiets behandling af oplysninger gælder endvidere lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger.

I den danske straffeprocessuelle teori har Hans Gammeltoft-Hansen defineret et »tvangsindgreb« som »en foranstaltning, der efter sit almindelige formål udføres som led i en strafforfølgning, og hvorved der realiseres en strafbar gerningsbeskrivelse rettet mod legeme, frihed, fred, ære eller privat ejendomsret«.[5] Et tvangsindgreb kræver ifølge Gammeltoft-Hansen et klart hjemmelsgrundlag.[6] Gorm Toftegaard Nielsen har dog kritiseret definitionen ved blandt andet at henvise til, at det ikke er frugtbart at anskue politiets anvendelse af tvangsindgreb ud fra den teoretiske synsvinkel, at politiet principielt begår forbrydelser.[7]

Til denne begrebsmæssige diskussion kan anføres, at der ikke ses at være uenighed mellem Gammeltoft-Hansen og Toftegaard Nielsen om, at politiet som en forvaltningsmyndighed er undergivet det almindelige hjemmelskrav.[8] Som en kvalificering af politiets mange, forskellige efterforskningsmetoder, har Gammeltoft-Hansens definition af et tvangsindgreb været et vigtigt bidrag til at indkredse, hvor politiets efterforskning er mest indgribende over for borgeren, og hvor der må kræves en klar lovhjemmel.[9] Således ses definitionen anvendt i Strafferetsplejeudvalgets betænkninger som et begrebsmæssigt udgangspunkt ved reguleringen af nye efterforskningsmetoder.[10]

Den danske diskussion om definition af et tvangsindgreb må nu siges til en vis grad at være overhalet af udviklingen i regi af Den Europæiske Menneskerettighedskonvention,[11] hvor artikel 8 foreskriver, at myndighedernes indgreb i borgerens privatliv, familieliv, hjem og korrespondance kun må ske, hvis indgrebet er foreskrevet ved lov og er nødvendigt i et demokratisk samfund blandt andet af hensyn til at forebygge forbrydelser. Det følger af praksis fra Den Europæiske Menneskerettighedsdomstol, at der stilles skærpede krav til hjemmelens klarhed, når der er tale om alvorlige indgreb, såsom ransagning og beslaglæggelse, hvilket er udtrykt i dommen, *Petri Sallinen og andre mod Finland*: »*The Court would emphasise that search and seizure represent a serious interference with private life, home and correspondence and must accordingly be based on a »law« that is particularly precise. It is essential to have clear, detailed rules on the subject.*«.[12] Ligeledes, når der er tale om hemmelige indgreb, eksempelvis i meddelelseshemmeligheden.[13]

Politiets efterforskning i en digital kontekst må således grundlæggende anskues ud fra, om politiet tilgår offentligt tilgængelige oplysninger, eller om politiet skaffer sig adgang til borgerens data i et privat informationssystem. Såfremt politiet ved hjælp af »hacking«-metoder får adgang til private data, vil dette – både efter Gammeltoft-Hansens definition af straffeprocessuelle tvangsindgreb og efter EMRK artikel 8 om indgreb i privatliv mv. – kræve klar lovhjemmel.

I internettets mangfoldighed af hjemmesider, sociale platforme, datalagre, servere og datasystemer kan det være vanskeligt at gennemskue, hvornår man i den digitale verden befinder sig på offentligt tilgængeligt »område«, og hvornår man har bevæget sig ind på privat, beskyttet »område«. Et vigtigt pejlemærke for politiets skelnen mellem offentlige og private områder på internettet kan findes i straffelovens § 263, stk. 2, som regulerer, hvornår borgeren ifalder straf for at skaffe sig uberettiget adgang til andres oplysninger eller programmer i et informationssystem. Centralt er det her, at der ikke af bestemmelsen kan udledes noget krav om, at adgangen skal være sket ved, at en sikkerhedsforanstaltning er overvundet, hvorfor bestemmelsen dækker bredere, end populærbetegnelsen »hacking« antyder. Det afgørende er alene, om man har skaffet sig »uberettiget adgang«.[14]

I forhold til politiets mere konkrete »hacking«-metoder har Inger Marie Sunde, professor ved Politihøgskolen i Oslo, beskrevet disse ud fra overordnet set to fremgangsmåder:[15]For det første de *udstyrsbaserede fremgangsmåder*, der enten kan være hardwarebaseret ved en fysisk installation på mistænktes computer, eller softwarebaseret, hvor et »spion«-program installeres i mistænktes computer eller på hans brugerkonto på internettet. For det andet de *informationsbaserede fremgangsmåder*, der ikke kræver brug af teknisk udstyr, men hvor der enten er tale om, at politiet er i stand til at logge sig på computeren eller brugerkontoen i stedet for den retmæssige ejer/bruger, eller at politiet forstår at udnytte sårbarheder i sikkerheden til at skaffe sig adgang. Ifølge Sunde forekommer også flere mellemformer, som kombinerer både den udstyrsbaserede og den informationsbaserede fremgangsmåde.

Sundes overordnede systematik synes fortsat at være dækkende, og uanset at norsk politi udgør konteksten, må det lægges til grund,

---

5 Hans Gammeltoft-Hansen: »*Straffeprocessuelle tvangsindgreb*«, 1981, s. 44-45, og »Om afgrænsningen af »straffeprocessuelle tvangsindgreb««, U 1979B1.

6 Hans Gammeltoft-Hansen: »*Straffeprocessuelle tvangsindgreb*«, 1981, s. 23 ff., og »Om afgrænsningen af »straffeprocessuelle tvangsindgreb««, U 1979B1 (1).

7 Gorm Toftegaard Nielsen: »*Straffesagens gang*«, 6. udgave, 2016, s. 84 ff. og »Hvad er et tvangsindgreb? Om straffeproces og forvaltningsret«, Juristen 2005, nr. 5, s. 153. Hertil Gammeltoft Hansen: »Om definitionen af straffeprocessuelle tvangsindgreb« i »*Jurist uden omsvøb - Festskrift til Gorm Toftegaard Nielsen*« (red. Annette Møller-Sørensen og Anette Storgaard), s. 139-148.

8 Hertil Gammeltoft Hansen: »Om definitionen af straffeprocessuelle tvangsindgreb« i »*Jurist uden omsvøb - Festskrift til Gorm Toftegaard Nielsen*« (red. Annette Møller-Sørensen og Anette Storgaard), s. 141 f.

9 For en sammenfatning af diskussionen om straffeprocessuelle tvangsindgreb, se Michael Kistrup, Jakob Lund Poulsen, Jens Røn og Thomas Rørdam: »*Straffeprocessen«*, 3. udgave, 2018, s. 443 ff.

10 Eksempelvis Betænkning nr. 1023/1984, s. 12 ff., og Betænkning 1298/1995, s. 12 f.

11 Inkorporeret i dansk ret ved lov nr. 285 af 29. april 1992.

12 *Petri Sallinen og andre mod Finland*, dom af 27.09.05, pkt. 90, se hertil Jon Fridrik Kjølbro: »*Den Europæiske Menneskerettighedskonvention for praktikere*«, 4. udgave, 2017, s. 763.

13 Se hertil bl.a. dommene *Malone mod Storbritannien*, dom af 02.08.84, pkt. 67-68, *Amann mod Schweiz*, dom af 16. februar 2000, pkt. 56, samt *Roman Zakharov mod Rusland*, dom af 4. december 2015, pkt. 229. Se endvidere Jon Fridrik Kjølbro:»*Den Europæiske Menneskerettighedskonvention for praktikere*«, 4. udgave, 2017, s. 763, samt Jacobs, White and Ovey: »*The European Convention on Human Rights*«, 7th edition, 2017, s. 410 ff.

14 Om anvendelsesområdet for straffelovens § 263, stk. 2, se Gorm Toftegaard Nielsen, Thomas Elholm og Morten Niels Jakobsen: *Kommenteret straffelov, speciel del*, 11. udgave, 2017, s. 507 ff., Knud Waaben/Lars Bo Langsted: »*Strafferettens specielle del*«, 6. udgave, 2014, s. 240 f., Jørn Vestergaard: »*Forbrydelser og andre strafbare forhold*«, 3. udgave, 2018, s. 279 ff., Helena Lybæk Guðmundsdóttirs ph.d.-afhandling *»Clarifying broad »hacking« statutes«*, Aalborg Universitet, 2015, samt Lene Wacher Lentz: »»Hacking« og det digitale privatliv«, Juristen nr. 4/2018, s. 141.

15 Inger Marie Sunde: »Dataavlesing« i Tidsskriftet Retfærd 35 2012, nr. 1/136.

at samme og lignende metoder også kan anvendes af dansk politi i forbindelse med strafferetlig efterforskning.

I denne artikel tages udgangspunkt i de tekniske »hacking«-metoder, som ud fra Sundes systematik vil være både de udstyrsbaserede og de informationsbaserede metoder. Således udelades i denne fremstilling mere svigagtige metoder, f.eks. hvor man på uretmæssigt grundlag formår at få systemets administrator til at give adgang. For borgeren vil sådan svigagtig adgang til et datasystem efter en konkret vurdering kunne udgøre en overtrædelse af § 263, stk. 2. Når samme metode anvendes af politiet som led i en efterforskning, rejses en problematik omkring den ikke-lovregulerede efterforskningsmetode »infiltration«, som af pladsmæssige hensyn ikke omfattes af denne artikels analyse.

I det følgende afsnit undersøges med afsæt i Højesterets kendelse, U 2012.2614 H, hvilken hjemmel der gælder for politiets »hacking«, hvorved anvendelsesområdet for de tre straffeprocessuelle tvangsindgreb fastlægges: Hemmelig ransagning, jf. retsplejelovens § 799, dataaflæsning, jf. § 791 b, og indgreb i meddelelseshemmeligheden, jf. § 780 ff.

3. Højesterets kendelse i U 2012.2614 H

Sagens omstændigheder var, at politiet under efterforskning af narkokriminalitet efter straffelovens § 191 havde foretaget telefonaflytning og derved fået kendskab til passwords til den mistænktes Facebook- og Messenger-profiler. Politiet havde foretaget en kortvarig aflæsning af Facebook-profilen for at konstatere, om der fortsat var adgang til profilen og anmodede om rettens godkendelse samt tilladelse til fortsat adgang. Hvor byretten og landsretten havde tilladt indgrebet som dataaflæsning, jf. retsplejelovens § 791 b,[16] nåede Højesteret frem til, at indgrebet havde karakter af gentagne hemmelige ransagninger, jf. § 799, hvorefter Højesteret tiltrådte både det godkendte indgreb, og dét indgreb, der var givet tilladelse til fremadrettet.[17]

Højesteret begrundede afgørelsen således: *»Politiets adgang til T's Facebook- og Messenger-profiler kan ske fra en hvilken som helst computer med internetadgang alene ved hjælp af de koder, som politiet er blevet bekendt med via telefonaflytninger. De oplysninger, som politiet kan få kendskab til ved indgrebene, er – på samme måde som afsendte og modtagne e-mails – ikke oplysninger, der er undervejs i en kommunikationslinje. Oplysningerne er lagret på profilerne og tilgængelige ved hjælp af koderne. Højesteret finder, at indgrebene har karakter af gentagne hemmelige ransagninger, som kan foretages med hjemmel i retsplejelovens § 793, stk. 1, nr. 1, jf. § 799.«*

For Højesteret havde anklagemyndigheden påstået indgrebet tilladt efter reglerne om hemmelig ransagning, subsidiært som dataaflæsning. Højesteret tog anklagemyndighedens principale påstand til følge, og begrundelsen indeholder ingen bemærkninger, der relaterer sig til dataaflæsning.

Af hensyn til dommens præcedens havde det været interessant, om anklagemyndigheden havde nedlagt sine påstande i omvendt rækkefølge: Principalt påstået indgrebet henført under reglerne om dataaflæsning, med en subsidiær påstand om tilladelse af indgrebet som hemmelig ransagning. Dette skyldes, at reglerne om dataaflæsning er mindre restriktive end reglerne om gentagen hemmelig ransagning. Således kræver dataaflæsning, at der er tale om efterforskning af forbrydelser, der kan straffes med fængsel i 6 år eller derover, hvorimod hemmelig ransagning kun må finde sted ved ganske få specifikke, alvorlige forbrydelser, såsom terror, drab, narkotikakriminalitet mv. Derudover havde det været interessant, om Højesteret havde kunnet tage stilling til, om reglerne om dataaflæsning var anvendelige i en sådan situation, måske som den teknologisk mest præcise hjemmel til indgrebet.

3.1. Sondringen mellem ransagning og indgreb i meddelelseshemmeligheden

Højesterets vurdering af, om oplysningerne var undervejs i en kommunikationslinie, henviser til en traditionel, straffeprocessuel sondring mellem ransagning og indgreb i meddelelseshemmeligheden:[18] Beror oplysningerne hos enten afsenderen eller modtageren af meddelelsen, hvor politiet selv kan skaffe sig adgang til dem, er der tale om ransagning, eksemplificeret ved at politiet med rette nøgle kan låse en postboks op. Er der i stedet tale om meddelelser undervejs i en kommunikationslinie mellem afsender og modtager, hvor politiet får bistand fra teleudbyderen eller postvirksomheden til at gøre sig bekendt med meddelelsen, er indgrebet omfattet af reglerne om indgreb i meddelelseshemmeligheden.

I den digitale verden flyder disse to indgreb imidlertid sammen, navnlig i de tilfælde, hvor politiet gentagne gange, måske kontinuerligt, tilgår en online-profil, hvilket til forveksling ligner en aflytning af en kommunikation, hvor man i realtid aflytter/aflæser meddelelser samtidig med, at de bliver afgivet. Resultatet af de to indgreb – politiets kendskab til oplysningerne – kan være helt den samme.[19]

Tilbage af sondringen mellem ransagning og indgreb i meddelelseshemmeligheden i den digitale verden vil være, hvorvidt politiet selv kan tilgå oplysningerne (ransagning), eller om indgrebet kræver bistand fra en tjenesteudbyder (meddelelseshemmeligheden).

3.2. Anvendelsesområdet for dataaflæsning

Efter Højesterets kendelse i U 2012.2614 H er spørgsmålet, hvilket anvendelsesområde der så efterlades til reglerne om dataaflæsning.

Dataaflæsning er reguleret i retsplejelovens § 791 b som »aflæsning af ikke offentligt tilgængelige oplysninger i et informationssystem ved hjælp af programmer eller andet udstyr«. Bestemmelsen blev indført ved lov nr. 378 af 6. juni 2002 som reaktion på U 2001.1276 H, hvor politiet anmodede om rettens tilladelse til at installere et »snifferprogram« i en mistænkts computer, for at politiet kunne gøre sig bekendt med, hvad der blev skrevet på computeren, der var installeret i en lejlighed. Hvor byretten og landsretten havde vurderet indgrebet i forhold til observationsreglerne i § 791 a, stk. 3, nåede Højesteret imidlertid frem til, at den ønskede foranstaltning mest nærliggende måtte ligestilles med gentagen, hemmelig ransagning, hvilket der ikke var hjemmel til i retsplejeloven på daværende tidspunkt. Politiets anmodning om at installere »snifferprogrammet« blev derfor afvist.[20]

Den fremgangsmåde, der reguleres i bestemmelsen, er i forarbejderne beskrevet således: »dataaflæsning af computere mv.

---

16 Byrettens og landsrettens præmisser fremgår ikke af referatet i U 2012.2614 H.

17 Om afgørelsen se endvidere Lene Wacher Lentz: »Hemmelig ransagning og brevstandsning i den digitale virkelighed«, Juristen nr. 1/2016, s. 3.

18 Denne sondring fremgår af Betænkning nr. 1023/1984, pkt. 2.6.2. og videreføres i Betænkning 1377/1999, pkt. 6.1. pkt. 3.1. Se endvidere Lene Wacher Lentz: »Retsplejelovens regulering af politiets adgang til teledata«, Tidsskrift for Kriminalret, nr. 10/2017, pkt. 3.1.

19 Lene Wacher Lentz: »Hemmelig ransagning og brevstandsning i den digitale virkelighed«, Juristen nr. 1/2016, s. 10.

20 Om dataaflæsning se endvidere Lene Wacher Lentz: »Hemmelig ransagning og brevstandsning i den digitale virkelighed«, Juristen nr. 1/2016, s. 8 ff.

i medfør af bestemmelsen kan ske ved hjælp af teknisk udstyr, der fysisk installeres i computeren, eller i det omfang dette er teknisk muligt, ved at edb-programmer eller lignende sendes til den pågældende computer.«[21] Fokus er dermed på installering af program i en konkret computer, hvilket også ses af § 791b, stk. 3, hvorefter det i rettens kendelse om dataaflæsning skal anføres, hvilket informationssystem, indgrebet angår. Ifølge forarbejderne tænkes her på en computer eller lignende databehandlingsanlæg, og det anføres, at såfremt det ikke er muligt for politiet at give nærmere oplysninger om edb-udstyrets fabrikat, nummer eller lignende, der entydigt kan identificere dette, kan i stedet anføres et edb-udstyr, der benyttes på et bestemt, nærmere afgrænset sted, ligesom en computer kan identificeres som den bærbare computer, der tilhører den mistænkte.[22]

Retspraksis kan ikke bidrage til større klarhed om anvendelsesområdet for dataaflæsning, idet der af trykt retspraksis umiddelbart kun ses U 2012.2614 H – hvor Højesteret netop ikke anvendte bestemmelsen om dataaflæsning. Således er det ikke muligt til området for dataaflæsning at føje flere variationer og nuancer over konkrete metoder, hvilket er bemærkelsesværdigt navnlig i lyset af den hengåede tid siden bestemmelsens indførelse i 2002 og den hastige teknologiske udvikling og de muligheder, som internettet har givet.

Uagtet dataaflæsning ikke har resulteret i trykt retspraksis, er der dog ingen tvivl om, at indgrebet anvendes i praksis. Således har Politiets Efterretningstjeneste i forbindelse med evaluering af Terrorpakke I og II tilkendegivet, at man anvender dataaflæsning i mange tilfælde, og at dataaflæsning har vist sig at være et særdeles nyttigt efterforskningsmiddel og bl.a. er anvendt i forhold til målpersonerne i terrorsagerne, Vollsmose-sagen og Glasvej-sagen.[23]

Efter Højesterets kendelse i U 2012.2614 H er anvendelsesområdet for dataaflæsning formentlig alene den specifikke situation, bestemmelsen oprindeligt var møntet på: hvor politiet installerer et konkret spionprogram, som fortløbende videresender information om aktiviteten til politiet, enten ved at politiet har fået fysisk adgang til at installere programmet på computeren, eller at politiet har sendt programmet til computeren og derved muliggjort installationen. Disse *udstyrsbaserede* metoder må i lyset af internettets udbredelse og onlinemuligheder for fjernadgang til informationssystemer antages kun at udgøre en del af de praktiske »hacking«-værktøjer, politiet kan gøre brug af.

Navnlig de af Sunde nævnte *informationsbaserede fremgangsmåder*, der ikke kræver brug af teknisk udstyr, men hvor politiet på forskellig vis er i stand til at logge på computere eller systemer i stedet for den retmæssige bruger, som det skete i U 2012.2614 H, eller hvor politiet udnytter konkrete sårbarheder i datasystemer til at få adgang, synes ikke omfattet af anvendelsesområdet for bestemmelsen om dataaflæsning. Dette vil i stedet være hemmelig ransagning.

Hvilken lovhjemmel der dækker politiets »hacking« vil således bero på en nærmere vurdering af hvilke programmer og metoder, politiet gør brug af.

Det er imidlertid ikke hensigtsmæssigt, at kvalificering af indgrebet beror på en større teknisk udredning, når der meget ofte vil være tale om et hastende efterforskningsskridt, og indgrebet i borgerens digitale privatliv vil være det samme uanset metoden. Derudover er det svært at se begrundelsen for, at den situation, hvor politiet anvender eller gætter rette kode til f.eks. Facebook, er underlagt reglerne om hemmelig ransagning med det meget begrænsede anvendelsesområde, hvorimod politiets installering af programmer direkte på en computer kan anvendes i videre omfang efter reglerne om dataaflæsning.

Dog resterer fortsat det forbehold, at det ikke vides, hvordan Højesteret i U 2012.2614 H ville have vurderet situationen, hvis dataaflæsning i stedet for hemmelig ransagning havde været den principale påstand. Ville Højesteret have tilladt indgrebet med hjemmel i reglerne om dataaflæsning? Spørgsmålet vil næppe blive besvaret. Det kan konstateres, at der ikke ses trykt retspraksis, der kan ændre eller nuancere billedet af politiets hjemmel til »hacking«. Derimod er det forventeligt, at politi og anklagemyndighed afstemmer en sådan efterforskning med reglerne om gentagen, hemmelig ransagning, hvorfor en tilsvarende sag for Højesteret, hvor problematikken sættes på spidsen, næppe vil forekomme. Skal anvendelsesområdet for dataaflæsning og hemmelig ransagning justeres, vil dette kræve lovgivers medvirken.

4. Politiets »hacking«-hjemmel

Højesterets kendelse i U 2012.2614 H er skelsættende, idet hemmelig ransagning herefter fremstår som politiets almindelige hjemmel til »hacking«, dvs. når politiet med egne metoder kan få adgang til et informationssystem, og når adgangen ikke sker som dataaflæsning ved installation af et program på en konkret computer. I de filfælde, hvor politiet får bistand af en serviceudbyder til at få adgang til en kommunikation, f.eks. ved aflytning af en e-mail- eller chat-kommunikation, vil der være tale om indgreb i meddelelseshemmeligheden, jf. retsplejelovens § 780 ff.

4.1. Politiets »hacking« i sager om it-kriminalitet

Som tidligere nævnt er der forskel i anvendelsesområdet for hemmelig ransagning og dataaflæsning. Det følger af retsplejelovens § 799, at hemmelig ransagning kan ske over for både mistænkte og ikke-mistænkte, jf. §§ 793-795, i efterforskningen af sager om overtrædelse af straffelovens kapitel 12 eller 13, eller såfremt der er tale om en overtrædelse af nærmere angivne bestemmelser, blandt andet grov brandstiftelse (straffelovens § 180), grov narkotikakriminalitet (§ 191), drab (§ 237) og som de eneste berigelsesforbrydelser, de grove tyverisager (§ 286, stk. 1, jf. § 276), røveri (§ 288) og groft skattesvig (§ 289).

Som det ses, er der ikke hjemmel til hemmelig ransagning i efterforskning af it-kriminalitet, såsom »hacking« (§ 263, stk. 2), bedrageri på nettet (§§ 279 og 279 a) og udbredelse af overgrebsmateriale mod børn (§ 235), selv om det netop er ved it-kriminalitet, at politi-»hacking« kunne være særlig relevant.

Anderledes ved dataaflæsning, som kan ske i efterforskning af forbrydelser, som kan straffes med mere end 6 års fængsel, jf. retsplejelovens § 791 b, og indgreb i meddelelseshemmeligheden i form af aflytning, som også kan ske ved forbrydelser, der kan straffes med mere end 6 års fængsel eller hvis efterforskningen angår en af de nærmere opregnede forbrydelser i § 781.

I efterforskningen af sager om it-kriminalitet, eksempelvis »hacking« under skærpende omstændigheder, jf. straffelovens § 263, stk. 3, jf. stk. 2, vil der derfor være hjemmel til, at politiet med teleudbyderens eller internetudbyderens bistand aflytter en telefon- eller internetkommunikation, jf. retsplejelovens § 780, stk. 1, nr. 1, jf. § 781. I samme sag vil der være hjemmel til dataaflæsning ved at politiet installerer et spionprogram på den konkrete computer,

21 LFF 2001-12-13, nr. 35, de specielle bemærkninger til lovforslagets § 791 b (lov nr. 378 af 6. juni 2002).

22 LFF 2001-12-13, nr. 35, de specielle bemærkninger til § 791 b (lov nr. 378 af 6. juni 2002).

23 »Justitsministeriets redegørelse om erfaringerne med lovgivning indført i forbindelse med anti-terrorpakke I fra 2002 og anti-terrorpakke II fra 2006«, fra 2010, s. 26.

jf. § 791 b. Men der vil ikke være hjemmel til, at politiet skaffer sig adgang til datasystemet på anden vis, eksempelvis med de af Sunde nævnte *informationsbaserede* fremgangsmåder, når der ikke er hjemmel til hemmelig ransagning, jf. § 799.

Processuelt er de tre indgreb - hemmelig ransagning, indgreb i meddelelseshemmeligheden og dataaflæsning - underlagt samme krav, således krav om rettens kendelse, medmindre øjemedet forspildes, hvorefter indgrebet skal forelægges for retten inden 24 timer, ligesom der skal beskikkes en indgrebsadvokat. Fælles er også, at indgrebene kun tillades i fire uger ad gangen, med mulighed for forlængelse, ligesom reglerne om senere underretning af de berørte er de samme.[24]

4.2. Retspolitiske overvejelser

Det er nu over fem år siden Højesterets kendelse, og der har ikke været nogen tiltag fra lovgivers side til at ændre på denne retstilstand. Det sker ikke ofte, at Højesteret tager stilling til nye efterforskningsmetoder, og en afgørelse fra landets øverste retsinstans burde kalde på refleksion i forhold til afgørelsens præcedens og samspil med andre indgreb. Hemmelig ransagning er en af de mest restriktive hjemler i retsplejelovens katalog over tvangsindgreb, hvilket beror på, at metoden traditionelt har været anvendt til hemmelig ransagning af husrum mv., hvilket selvsagt må opleves som indgribende af de berørte. Spørgsmålet er, om politiets hemmelige adgang til digitale systemer opleves nær så indgribende.

Der synes at være behov for en præcisering af anvendelsesområdet for dataaflæsning. Meget taler for at lade dataaflæsning være hjemmel for den digitale aflæsning af data og beskeder i informationssystemer, som politiet selv kan foretage uden udbyderens medvirken, og dermed lade sådanne indgreb udgå af anvendelsesområdet for hemmelig ransagning.

Ved en nyaffattelse af bestemmelsen om dataaflæsning kunne det overvejes at sondre mellem de forskellige former for digitale systemer, som politiet tillades adgang til. Data i en computer, en mobiltelefon eller en virksomheds intranet synes mere privat, end den blotte adgang til en konkret brugerprofil på de sociale medier, hvor brugeren ved oprettelsen af profilen har givet samtykke til, at platformen kan monitorere brugerens data og adfærd, og i vidt omfang videregive data til en bred kreds af annoncører, samarbejdsparter, retshåndhævende myndigheder mv. Færden på de sociale medier synes således ikke at give den samme berettigede forventning om privatliv som beskyttelsen af hjemmet, en konkret computer mv.

Ved beskrivelsen af politiets metoder til dataaflæsning og hvilke private data og systemer, der er omfattet af reguleringen, må findes en balance mellem på den ene side at sikre en tilstrækkelig præcision, således at bestemmelsen er praktisk anvendelig, og på den anden side at anvende begreber, som også fremtidige teknologiske nyskabelser i et vist omfang kan rummes i.

Vigtigt er det at sikre en overensstemmelse med reglerne om indgreb i meddelelseshemmeligheden, idet dataaflæsning har samme virkning som aflytning af en kommunikation, blot med den forskel, at det er politiet og ikke udbyderen, der udfører indgrebet. Bedst stemmende ville således være at fastholde samme kriminalitetskrav på 6 års fængsel.

5. Undersøgelse af beslaglagt computer eller telefon

Politiets hemmelige adgang til private datasystemer er, som det ses, restriktivt reguleret. I det følgende behandles den situation, hvor politiet ved undersøgelse af en beslaglagt computer eller telefon i realiteten vil være i stand til at foretage det samme indgreb. Ved undersøgelsen kan politiet få adgang til online-profiler mv., hvorved det er muligt at etablere en fremadrettet, online-overvågning, hvilket aktualiserer spørgsmålet, om der herved indledes en hemmelig ransagning. Situationen er ikke reguleret i retsplejeloven, og retstilstanden er i høj grad uklar.

5.1. Beslaglæggelsen

En computer eller mobiltelefon, som en mistænkt har rådighed over, kan beslaglægges efter retsplejelovens § 802, stk. 1, hvis den pågældende person med rimelig grund er mistænkt for en lovovertrædelse, der er undergivet offentlig påtale, og der er grund til at antage, at genstanden kan tjene som bevis eller bør konfiskeres, eller ved lovovertrædelsen er fravendt nogen, som kan kræve den tilbage. I samme situationer vil beslaglæggelse kunne ske hos ikke-mistænkte, jf. § 803. Det følger af § 805, at beslaglæggelse ikke må foretages, hvis indgrebet står i misforhold til sagens betydning og det tab eller den ulempe, som indgrebet kan antages at medføre.

Retten træffer afgørelse om beslaglæggelse, jf. § 806, stk. 1, politiet gennemfører indgrebet og foreviser retskendelsen for den, beslaglæggelsen retter sig imod, jf. § 807, stk. 1. Denne fremgangsmåde forudsætter, at politiet ved præcis, hvilke genstande, der skal beslaglægges og hvem, der har rådighed over dem.

I forhold til den i praksis ofte forekommende situation, hvor der under ransagning fremfindes genstande, der er relevante at beslaglægge, kan politiet træffe afgørelse om beslaglæggelse på stedet, hvis indgrebets øjemed ellers ville forspildes, jf. § 806, stk. 4. Den, der er berørt af indgrebet, kan anmode om, at sagen indbringes for retten, hvorefter politiet snarest muligt og senest inden 24 timer forelægger sagen for retten, der afgør, om indgrebet kan godkendes. Politiet skal vejlede mistænkte om denne mulighed, jf. § 807, stk. 1. Såfremt den, som indgrebet retter sig imod, meddeler skriftligt samtykke til indgrebet, kan politiet træffe afgørelse om beslaglæggelse udenretligt, jf. § 806, stk. 8.

Som det ses, er betingelserne for beslaglæggelse forholdsvis milde, idet der ikke er krav til kriminalitetens grovhed, og indgrebet vil derfor også kunne ske i sager med påstand om bødestraf.

Der er mulighed for, at beslaglæggelsen kan foregå hemmeligt, og dermed uden at den mistænkte eller andre gøres bekendt med indgrebet, hvis dette er af afgørende betydning for efterforskningen, jf. retsplejelovens § 807 e.[25] Her ses ikke, at kravene til kriminalitetens grovhed eller mistankens styrke er skærpet.

Ved bestemmelsens tilblivelse var i det oprindelige forslag til § 807 e en formulering: »Hvis det er af afgørende betydning for efterforskningen, at der i forbindelse med en ransagning efter § 799, stk. 1, foretages beslaglæggelse, uden at den mistænkte eller andre gøres bekendt hermed...«[26] Således var den oprindelige forudsætning for hemmelig beslaglæggelse, at der forud var gået en hemmelig ransagning, og at de restriktive betingelser herfor var opfyldt.

I forbindelse med Retsudvalgets behandling af lovforslaget indgik et ændringsforslag fra Justitsministeriet om, at henvisningen til hemmelig ransagning skulle udgå.[27] Baggrunden var, at

24 Retsplejelovens § 791 b, stk. 3 og 4, § 799, stk. 2, samt § 783, § 784 og § 788.

25 Indført ved lov nr. 1552 af 21. december 2010. Ifølge lovforslaget var hensigten at sikre en udtrykkelig hjemmel til hemmelig beslaglæggelse (LFF2010-11-10, nr. 54), pkt. 4.

26 LFF2010-11-10, nr. 54 (lov nr. 1552 af 21. december 2010).

27 LFB 2010-12-09, nr. 54 (lov nr. 1552 af 21. december 2010).

Rigsadvokaten over for Justitsministeriet havde oplyst, at det ville kunne være relevant for politiet under efterforskningen at foretage hemmelig beslaglæggelse, uden at det skete i forbindelse med en hemmelig ransagning. Der kunne bl.a. være tale om tilfælde, hvor der skete beslaglæggelse i form af kopi af dokument indeholdende oplysninger om f.eks. kriminelle grupperingers medlemsliste og planer, og hvor det kunne være relevant for efterforskningen at kunne beslaglægge hemmeligt.

Justitsministeriets ændringsforslag blev vedtaget, og den nugældende bestemmelse indeholder ingen henvisning til en forudgående hemmelig ransagning.

Det hemmelige ved beslaglæggelsen modsvares af, at de processuelle regler fra indgreb i meddelelseshemmeligheden efter kapitel 71 finder anvendelse, således navnlig et krav om, at indgrebet *skal* indbringes for retten inden 24 timer, ligesom der er krav til varigheden af indgrebet, beskikkelse af en indgrebsadvokat, underretning af de berørte personer mv.[28]

5.2. Undersøgelse af det beslaglagte

Når retten har taget stilling til spørgsmålet om beslaglæggelse, eller ejeren af genstanden har afstået fra at indbringe beslaglæggelsen for retten, vil den beslaglagte genstand blive undersøgt af politiet alt efter formålet med indgrebet og den efterforskning, som beslaglæggelsen relaterer sig til. Efter rettens godkendelse af indgrebet, vil der i almindelighed være »arbejdsro« til politiets nærmere undersøgelse af genstanden, medmindre ejeren anfægter, hvad der skal undersøges og hvordan, hvilket kan nødvendiggøre rettens stillingtagen.

Et eksempel herpå var Højesterets stillingtagen til beslaglæggelse af computere og mobiltelefoner hos ugebladet, Se og Hør, U 2015.1249 H. Det måtte lægges til grund, at det beslaglagte materiale også indeholdt kildebeskyttede oplysninger uden relevans for efterforskningen, hvorfor disse oplysninger skulle frasorteres på en betryggende måde, jf. den særlige fremgangsmåde, der følger af retsplejelovens § 807, stk. 3, som gælder for redaktører og redaktionelle medarbejdere, jf. § 172. Højesteret fandt, at rettens gennemsyn af materialet af praktiske grunde skulle ske hos politiet med sagkyndig bistand af politiet og således, at anklagemyndigheden og selskabet, som ejer af materialet, havde mulighed for at være til stede og udtale sig om, hvorvidt dokumenter kunne indgå i efterforskningen.

I Se og Hør-sagen godkendte Højesteret politiets almindelige fremgangsmåde om at lave en »spejling« af computerens indhold, således at dette fastholdes eller »fastfryses«, hvilket er en fordel under den tekniske undersøgelse. Dette sikrer, at tidsangivelser mv. forbliver korrekte, og at data ikke slettes uforsætligt under den tekniske undersøgelse. For ejeren vil spejling af computeren også være en fordel, idet politiet derved sikrer sig indholdet, hvorefter computeren ofte kan tilbageleveres, og indgrebet dermed ikke udstrækkes yderligere til gene for den pågældende.

Beslaglagte mobiltelefoner udlæses, men synes ikke at blive tilbageleveret i samme omfang undervejs i efterforskningen, som det sker med computere. Ofte vil der være en konkret grund til dette, såsom at mistænkte er varetægtsfængslet og derfor ikke skal have sin mobiltelefon til rådighed, eller at politiet ønsker at kontrollere og styre kommunikationen mellem flere involverede mistænkte i en efterforskning. Den væsentligste forskel på computere og mobiltelefoner er imidlertid, at mobiltelefoner fortsat har signal og derfor kan være »aktiv« under beslaglæggelsen og dermed til stadighed aktuel og relevant i forhold til efterforskningen, hvorimod dette som udgangspunkt ikke er tilfældet med en computer. Dette modificeres dog dels af, at det er muligt at ændre computerens indstillinger, så den tilgår politiets wifi-forbindelse, så computeren også bliver »aktiv« under beslaglæggelsen, dels at computere, iPads mv., kan have simkort, og dermed egen internetforbindelse.

For både computere og mobiltelefoner gælder altså, at disse kan være »aktive« under en beslaglæggelse, hvilket ud over undersøgelsen af indholdet i datasystemet, også giver mulighed for en fremadrettet, online-efterforskning.

Således kan det ske, at der i beslaglæggelses-perioden på mobiltelefonen indgår telefonopkald eller sms-beskeder, og for både computere og mobiltelefoner, at apps og browservinduer for email-konti, chats og sociale profiler åbnes og opdateres, med mulighed for, at politiet fremadrettet følger med i denne nye aktivitet. Dette aktualiserer spørgsmålet om, hvorvidt denne nye aktivitet kan rummes i beslaglæggelsen og den undersøgelse, der som led heri kan foretages, eller om der i stedet iværksættes en (ny og måske hemmelig) ransagning.

Forskellen i retsgrundlaget er markant: Enten gælder de meget milde betingelser for beslaglæggelse, hvorefter indgrebet kan foretages, hvis forholdet er undergivet offentlig påtale. Eller også gælder reglerne om ransagning, og i de tilfælde, hvor undersøgelsen må siges at være hemmelig, må indgrebet kun ske, hvis sagen angår en af de forbrydelser, der er nævnt i retsplejelovens § 799.

Konsekvensen ses også i den processuelle regulering: Hvis det lægges til grund, at situationen er omfattet af beslaglæggelsen, vil indgrebet uden videre kunne foretages. Lægges det derimod til grund, at der er tale om en ny ransagning, kræves, at retten tillader indgrebet ud fra en konkret vurdering af sagens omstændigheder, herunder af mistankens styrke, kriminalitetens karakter og omfang samt formålet med indgrebet og proportionaliteten herved, jf. retsplejelovens § 793 ff. Hvis ransagningen vurderes som hemmelig, følger som tidligere nævnt en række yderligere processuelle krav i form af indgrebsadvokat, underretning mv. Processuelt ses således ved en ny ransagning, og særligt ved hemmelig ransagning, en høj grad af beskyttelse af den berørte borgers interesser.

Retsplejeloven indeholder ingen bestemmelser om politiets undersøgelser af beslaglagte genstande. Hvordan en fremadrettet, onlineundersøgelse af beslaglagte computere og mobiltelefoner skal anskues, er uafklaret ud fra lovteksten, forarbejder og tilgængelige retningslinjer for politi og anklagemyndighed. Ej heller ses nogen retspraksis om det retlige grundlag for sådanne onlineundersøgelser ved hjælp af beslaglagte computere og mobiltelefoner.

I det følgende gøres nogle overvejelser for at kvalificere sådanne fremadrettede onlineundersøgelser.

5.3. Retlig kvalificering af »fremadrettet onlineundersøgelse«

Retsplejelovens straffeprocessuelle tvangsindgreb er overordnet set blandt andet reguleret ud fra, om de sker åbent i forhold til de berørte borgere, der f.eks. kan overvære en ransagning, hvilket er underlagt forholdsvis milde betingelser, eller om det sker hemmeligt, f.eks. ved hemmelig ransagning eller standsning af breve, hvilket er restriktivt reguleret.

En beslaglæggelse af en computer eller en mobiltelefon er som udgangspunkt et åbent indgreb med involvering af ejeren, men som det ses i det følgende, placerer den tekniske onlineundersøgelse sig i en gråzone mellem et åbent og et hemmeligt indgreb.

I den praktiske virkelighed kan der forekomme situationer, hvor en beslaglæggelse sker uden ejerens viden, f.eks. hvor telefonen

28 Retsplejelovens § 807 e, stk. 2.

er fundet på et gerningssted, og rette ejer endnu ikke er fundet, eller det har vist sig umuligt af forskellige årsager at komme i kontakt med vedkommende. Desuden kan konkrete omstændigheder begrunde, at en beslaglæggelse indtil videre holdes hemmelig, jf. § 807 e, f.eks. når ejeren indgår i et sagskompleks med flere mistænkte, hvor kommunikationen imellem dem kan være af betydning for sagens opklaring.

Selv om beslaglæggelse af computer eller telefon sker åbent med ejerens vidende, kan man ikke deraf udlede, at ejeren vil være fuldt ud vidende om, at politiet ved undersøgelsen af computeren eller telefonen skaffer sig adgang til apps, profiler på sociale medier mv. Hvor meget politiet fra den konkrete genstand kan få adgang til, vil afhænge af den konkrete installering, herunder af indlejrede adgangskoder i browseren og i apps. Ejeren kan forudsige, at computeren eller genstanden må blive undersøgt, men knap så oplagt er det for alle, at de brugerkonti og platforme »i skyen«, politiet også kan få adgang til, bliver omfattet.

Uanset de konkrete omstændigheder i forhold til ejeren af telefonen, er der også ved en fremadrettet, onlineovervågning et hensyn at tage til tredjemand, der ved at ringe, maile, chatte eller på anden vis får sin kommunikation og sit privatliv viklet ind i politiets efterforskning.

Den konkrete undersøgelse kan dermed være meget svær at rubricere i forhold til, om der er tale om et åbent indgreb, som ejeren af mobiltelefonen eller computeren er bekendt med og måske endda har samtykket i, eller om indgrebet holdes hemmeligt for en eller flere af de berørte personer, hvilket taler for, at indgrebet kvalificeres som en hemmelig ransagning.

Sat på spidsen kan man forestille sig, at en mobiltelefon, der er beslaglagt i forbindelse med et indbrud, ligger på kriminalassistentens skrivebord frem til hovedforhandlingen, hvor der i den mellemliggende periode kan holdes øje med indgående telefonopkald og sms, ligesom det er muligt at tilgå personens brugerprofiler på diverse virtuelle kommunikationsplatforme. Hvis der allerede er sikret bevis for indbruddet, er det så lovligt uden konkret mistanke, at følge med i telefonens kommunikation og aktivitet? Har det nogen betydning, om politiet »holder udkig« efter flere og måske bedre beviser for indbruddet, eller om man ser efter beviser, der relaterer sig enten til andre personer eller til et nyt strafbart forhold, som politiet så kan indlede en efterforskning af? Og hvor længe må denne overvågning i så fald vare?

En undersøgelse af computeren eller telefonen for et helt andet strafbart forhold strider mod retsplejelovens grundtanke om, at et indgreb mod borgeren kræver en konkret mistanke, og at der er et efterforskningsmæssigt formål med indgrebet. Dette udgangspunkt støttes af de almindelige forvaltningsretlige principper om saglighed og proportionalitet ved myndighedsudøvelsen.

Uagtet disse grundlæggende principper, er udfordringen blot, at grænsen er meget flydende for, hvornår man undersøger en allerede etableret mistanke, og hvornår man »leder efter« et nyt strafbart forhold.

Skulle det ske i eksemplet med mobiltelefonen på kriminalassistentens skrivebord, at der indgår beviser for et nyt strafbart forhold, er spørgsmålet, hvordan disse beviser må bruges i strafforfølgningen mod ejeren, hvilket knytter an til begrebet tilfældighedsfund, som behandles i det følgende.

5.4. Tilfældighedsfund

Tilfældighedsfund vedrører den situation, hvor der er hjemmel til indgrebet på baggrund af en mistanke om en konkret forbrydelse, men hvor der ved udførelsen af indgrebet fremkommer beviser for et andet strafbart forhold. Sådanne tilfældighedsfund er reguleret for indgreb i meddelelseshemmeligheden i retsplejelovens § 789 og i relation til ransagninger i § 800.[29]

Reglerne er udtryk for en afvejning mellem to hensyn: På den ene side at kunne anvende beviser i straffesager for at nå frem til det materielt sande resultat, uanset hvordan beviserne fremkommer. På den anden side, at politiet ikke skal kunne »oppuste« en mistanke for en forbrydelse, der kan opfylde betingelserne for indgrebet, mens der reelt søges efter beviser for en mindre forbrydelse, der ikke selv kunne danne grundlag for indgrebet.[30]

Ved tilfældighedsfund er grundlaget for at tilvejebringe beviserne lovligt, man finder blot noget andet, end det man leder efter. Således ikke at forveksle med ulovligt tilvejebragte beviser, hvor der ikke er et lovligt indgreb til at indhente beviserne, f.eks. hvis der er iværksat en aflytning i en sag, som ikke opfylder kriminalitetskravet i § 781. Anvendelse af ulovligt tilvejebragte beviser er ikke lovreguleret, men vil kun kunne anvendes i en hovedforhandling, hvis retten konkret tillader det.[31]

Det følger af § 800, stk. 1, at tilfældighedsfund fra en ransagning frit kan anvendes som led i politiets efterforskning, men at tilfældighedsfund ikke må anvendes som bevis i retten, medmindre oplysningerne angår en lovovertrædelse, der i sig selv kunne have dannet grundlag for indgrebet. Dette stemmer overens med U 2012.1045 Ø, hvor der i udførelsen af en ransagning i relation til hæleri opstår mistanke om besiddelse af narkotika, hvorved ransagningen udvides til også at omfatte dette forhold. En sådan »udvidelse« af efterforskningen på stedet er uproblematisk, når det nye forhold i sig selv kunne give anledning til ransagningen.[32]

I de tilfælde, hvor tilfældighedsfundet ikke selv kunne have begrundet indgrebet, er der dog mulighed for, at retten konkret kan tillade, at tilfældighedsfundet anvendes som bevis, hvis betingelserne herfor er opfyldt, jf. § 800, stk. 2.

Ifølge Strafferetsplejeudvalgets Betænkning 1159/1989 om ransagning, som dannede grundlag for lovforslaget til § 800, var det udvalgets opfattelse, at ved alle straffeprocessuelle tvangsindgreb hvor tilfældighedsfund kunne forekomme, skulle retstilstanden være som ved § 789 om tilfældighedsfund fra indgreb i meddelelseshemmeligheden, om at tilfældighedsfund fra indgreb i hovedreglen kun må anvendes, hvis de angår en forbrydelse, der selv kunne give anledning til samme indgreb.[33]

Bestemmelsen i § 800 angår efter sin ordlyd alene ransagninger, og det kan diskuteres, hvorvidt den er dækkende for tilfældighedsfund, der fremkommer ved en teknisk undersøgelse af beslaglagte genstande uden forudgående ransagning, for eksempel når mobiltelefonen er fundet af politiet på gerningsstedet. Sådanne

29 Se hertil Hans Gammeltoft-Hansen: *»Straffeprocessuelle tvangsindgreb«*, 1981, s. 205 ff., Strafferetsplejeudvalgets Betænkning 1023/1984 om indgreb i meddelelseshemmeligheden, s. 110 ff., Strafferetsplejeudvalgets Betænkning 1159/1989 om ransagning under efterforskning, pkt. 5.3., samt Michael Kistrup, Jakob Lund Poulsen, Jens Røn og Thomas Rørdam: *»Straffeprocessen«*, 3. udgave, 2018, s. 469 f. og 491.

30 Betænkning 1023/1984, s. 113.

31 Om ulovligt tilvejebragte beviser se bl.a. Michael Kistrup, Jakob Lund Poulsen, Jens Røn og Thomas Rørdam: *»Straffeprocessen«*, 3. udgave, 2018, s. 678 ff.

32 Michael Kistrup, Jakob Lund Poulsen, Jens Røn og Thomas Rørdam: *»Straffeprocessen«*, 3. udgave, 2018, s. 491.

33 Strafferetsplejeudvalgets Betænkning 1159/1989 om ransagning under efterforskning, pkt. 5.3. samt lovforslaget, LFF 1996-11-28, nr. 98, pkt. 5.3.7. (lov nr. 411 af 10. juni 1997).

situationer er dog meget sammenlignelige med ransagninger, og det er mest sandsynligt, at tilfældighedsfund fra tekniske undersøgelser af computere eller mobiltelefoner vil være omfattet af § 800 eller dennes analogi.

5.5. Retlig regulering

Både hemmelig ransagning og dataaflæsning er underlagt både materielt og processuelt en ganske restriktiv regulering. Som det fremgår, kan samme metoder i realiteten anvendes med beslaglagte computere og mobiltelefoner, hvor mailsystemer, brugerkonti og private informationssystemer også kan tilgås, overvåges og aflæses hemmeligt i en længere periode fremadrettet.

Det er svært at vurdere, i hvilket omfang sådanne fremadrettede onlineundersøgelser i praksis forekommer. Man må bare konstatere, at muligheden er nærliggende, når man først har adgang til den mistænktes computer eller mobiltelefon, og der er et stort bevismæssigt potentiale i at kunne dokumentere den mistænktes kommunikation med medgerningsmænd mv.

Med forbehold for eventuelle mundtlige anvisninger internt i politi og anklagemyndighed, synes der i fraværet af en egentlig regulering at være risiko for, at denne form for efterforskning anvendes og først bliver beskrevet i politirapporter, hvis politiet faktisk finder noget, man ønsker at gøre brug af som bevis i en straffesag. I sådanne tilfælde vil det kræve et større arbejde for forsvareren at sætte sig ind i, præcis hvornår beviset er tilvejebragt, og hvor længe overvågningen via computeren eller telefonen i realiteten har pågået. Uanset forsvarerens ihærdighed for at få dette belyst ud fra tilgængelige politirapporter og tekniske specifikationer, er det næppe umagen værd, når sådanne beviser i vidt omfang vil blive tilladt ført under hovedforhandlingen som følge af § 800 om tilfældighedsfund eller dennes analogi. Dette for at tilgodese hensynet til, at få den materielle sandhed frem om det forhold, der er rejst tiltale for.[34]

Når politiets hemmelige adgang til private data og systemer reguleres af de restriktive bestemmelser om hemmelig ransagning og dataaflæsning, må samme indgreb foretaget via beslaglagte computere eller mobiltelefoner også vurderes som en indgribende efterforskning mod den enkelte. Dette taler for en klar regulering i retsplejeloven. I den forbindelse må man bl.a. tage stilling til, hvor længe efter sikringen af genstanden, undersøgelsen kan foretages, hvor mange gange genstanden kan tilgås inden for en nærmere fastlagt periode, og hvorvidt undersøgelsen kan foretages offline eller online. Samtidig bør der tages stilling til anvendelse af tilfældighedsfund i disse situationer, så der også på dette punkt sikres klare juridiske rammer.

Ved samme lejlighed kunne det overvejes at regulere, om politiet må indtage en mere aktiv rolle i forhold til de beslaglagte mobiltelefoner og computere, f.eks. om politiet uden at give sig til kende som politimyndighed kan besvare telefonopkald, sms og mails eller overtage en profil på de sociale medier. Disse problematikker klinger an til efterforskningsmetoderne infiltration og agentvirksomhed og behandles ikke yderligere her.

6. Afrunding

Som nævnt indledningsvist kræver politiets indgreb i borgerens privatliv et klart hjemmelsgrundlag. Den teknologiske udvikling har medført, at en stor del af vores privatliv og kommunikation nu foregår digitalt, ligesom politiet har fået nye, sofistikerede, digitale værktøjer til rådighed. Denne digitale kontekst udfordrer den velkendte regulering i retsplejeloven af de straffeprocessuelle tvangsindgreb.

Politiet har ikke en egentlig hjemmel til »hacking«, men indgrebet reguleres i stedet af tre forskellige indgreb: hemmelig ransagning, dataaflæsning eller indgreb i meddelelseshemmeligheden. Samspillet mellem disse indgreb forekommer ikke hensigtsmæssigt, navnlig når sondringen mellem hemmelig ransagning og dataaflæsning, vil bero på en nøjere teknisk kvalificering af metoden, uagtet indgrebet i borgerens digitale privatliv kan være nøjagtig det samme. Det må ligge fast efter U 2012.2614 H, at politiets almindelige hjemmel til »hacking« udgøres af reglerne om hemmelig ransagning, hvilket ikke kan anvendes i efterforskning af it-kriminalitet.

Når hemmelig ransagning, i form af fremadrettet online-overvågning af digitale systemer, i realiteten kan ske ud fra beslaglagte computere og mobiltelefoner, er der også grund til at skabe en klar regulering af denne form for efterforskning, således at de berørte borgeres digitale privatliv i tilstrækkelig grad beskyttes.

34 Om sådanne problematikker, se Michael Kistrup, Jakob Lund Poulsen, Jens Røn og Thomas Rørdam: *»Straffeprocessen«*, 3. udgave, 2018, s. 27 f. og 678 ff.

