Efterforskning i den digitale verden

Kolbrún Benediktsdóttir, vicestadsadvokat, Island

Efterforskning i straffesager har ændret sig meget i de sidste år og årtier. Det er det mange grunder for men forandringer koblet til den digitale samfund spiller måske den største rolle. Men hvad betyder det? Vi står selvfølgelige fremfor nye typer av kriminalitet, især når det gjælder it-kriminalitet fordi at det findes jo altid dem som vil bruger ny teknologi til at begå forbrydelser. Men hvad er it-kriminalitet? Skal vi definere it-kriminalitet bredt eller snævert? Vi må passe på at vi ikke for hurtigt sætter en stempel på en adfærd som it-kriminalitet kun fordi at det er en tilslutning eller kobling til elektroniske medier. I dagens samfund har de fleste forbrydelser en ellar anden kobling til elektroniske medier og det er ikke altid nye typer sager men måske kun nyt scenario eller nye udførelsesformer af kriminalitet. Referatet drøfter disse spørgsmål og andre relaterede og hvad den nye virkeligheden betyder for politi og anklagemyndigheder når det gjælder efterforskning i straffesager.

1. Indledning

Det kræver ikke mange ord at beskrive at vi lever i en digital tidsalder. En meget stor del af kommunikationen mellem folk foregår via nettet eller via anden slags teknisk udstyr. Vi sender e-mail, sms-besked, og sender besked via sociale netværk sådan som Facebook, Twitter, Snapchat, etcetera. Vi udfører vores bankforretninger igennem hjemmebanken og mange af os træder sjældent ind i en bankfilial. Varer købes i voksende grad via nettet og sådan kunne jeg blive ved med at remse op de utallige it-muligheder som står til rådighed. Dette er sådan set ikke noget nyt men dette eskalerer med en enorm fart og teknikken bliver stadig mere sofistikeret. Det er meget svært bare at holde os orienteret og endnu sværere at holde trit med udviklingen. Med den voksende tekniske udvikling ser vi også at en ny type kriminalitet er dukket op, *cyber crime*, som også kan kaldes it-kriminalitet eller digital kriminalitiet. Vi ser stadigt nye scenarier af denne type kriminalitet, og dette medfører at der må findes svar på en række spørgsmål med henblik på at kunne efterforske og retsforfølge denne kriminalitet. Man kan vistnok sige at næsten alle kriminelle handlinger som begås i

dag, er relateret til computere eller internettet på en eller anden måde. Overtrædelserne kan være begået ved brug af computere eller internettet, der kan spores bevismateriale inde i disse eller at overtrædelsen er rettet mod computere, netværker eller internettet. Dette er virkeligheden som politi og anklagemyndigheder står over for og den indebærer forskellige udfordringer for det efterforskningmæssige og retsforfølgningsmæssige arbejde. Disse myndigheder samt andre parter som er inddraget i behandling af straffesager i retssystemet må følge godt med i udviklingen som sker og retshåndhævelsessystemet må være parat til at træde ind og reagere raskt, fordi den digitale verden, ændres hurtigt og udvikles raskt. På hjemmesiden hos den danske rigsadvokat i februar fandtes en nyhed om hvordan en it-ingeniør i den danske rigspolitichefs nationale cyber crime enhed (Rigspolitiets Nationale Cyber Crime Center (NC3) havde for nylig gjort et gennembrud med en ny efteforskningsmetode som gør det muligt at afsløre de kriminelles transaktioner på det såkaldte mørkenet (Deep Web), hvor der foregår forskellig kriminalitet, som f.eks. nakotika- og våbenhandel, deling af pædofilbilleder, m.m. Det beskrives at denne nye metode nu allerede har ført til straffe i to narkosager i Danmark, og ligeledes er det beskrevet at denne metode har vakt genlyd hos politimyndigheder i en række lande.[1]

Selv om det er meget vigtig at der etableres specielle efterforskningsenheder for at efterforske kompleks og alvorlig cyber kriminalitet, så er det mindst lige vigtigt at alle dem som deltager i efterforskningsarbejdet er i besiddelse af grundlæggende viden for at efterforske kriminalitet som i nogen grad er knyttet til computere og internettet. Det indebærer efter min mening en bestemt fare hvis man begynder at klassificere for mange overtrædelser som cyber kriminalitet, selv om de har en vis relation til computere og internettet. Der er i mange tilfælde bare tale om et nyt scenario af kriminalitet, som det er mest naturligt af efterforske på traditionel måde. Jeg har den følelse at der nogle gange svæver omkring en bestemt tendens til at skubbe disse sager til siden med de argumenter at det er så svært af efterforske disse sager og at cyberkrimininalitetsenheden må tage sig af dem, fordi overtrædelserne er begået på nettet. Det er derfor vigtigt at politiet og anklagemyndighed følger godt med i udviklingen og udvider deres kundskaber på dette område. Andre som er deltagere i sagsbehandlingen af straffesager i retshåndshævelsessystemet, sådan som dommere og forsvarere, er også nødt til at holde sig ajour med udviklingen, for at kunne processere sagerne.

[1] http://www.anklagemyndighede.dk/nyheder/Sider/gennembrud-nye-beviser-ophaever-kriminelles-anonymitet-paa-moerkenettet.aspx. Gennemlæst den 26. februar 2017

2. Cyber kriminalitet – eller bare overtrædelser i den digitale verden?

Inden vi går videre er der god grund til at kigge nærmere på begrebet computerkriminalitet (IT-kriminalitet) eller cyber crime på engelsk. Begrebet *cyber crime* blev født sammen med internettets opståen. Men hvad betyder begrebet og hvilken slags kriminelle handlinger falder ind under det? Eller er det måske unødvendigt at gruppere kriminaliteten på denne måde? Det har været påpeget at muligvis vil præfiksen *cyber* i sammenhængen cybercrime være overflødig og falde bort lige som det er unødvendigt at fremhæve at biler kører uden hestekræfter (automobil) og at elektriske pærer kører på elekricitet (elektriske pærer).[2] Realiteten er simpelthen den at vi lever i en digital verden og dette gælder på alle menneskehedens områder, herunder kriminalitet, og at det ville eventuelt være mere naturligt at kalde dem kriminalitet i en digital verden eller digital crime.[3] Dette er efter min mening meget vigtigt fordi sådan som jeg har tidligere forklaret har der været en bestemt tendens til at ekspedere forskellige sager med den begrundelse at dette er „bare nogen cyber crime" og endda lade det skinne igennem at forholdet måske ikke er strafbart, fordi det fandt sted på nettet. Eksempler på dette er forskellige sexkrænkelser, bl.a. krænkelser som har fået betegnelsen *hævnporno (e. revenge porn)* men som kaldes almindeligvis i dag digitale sexkrænkelser. I det sidstnævnte begreb kristalliseres nemlig problemet. Vi har haft nogle tilfælde i Island hvor politiet har hentydet til anmeldere at det er næsten umuligt at foretage noget efterforskningsmæssigt over for billeder som har været lagt ud på nettet, distribueret via de sociale medier eller spredt på lignende måde. At dette var handlinger som ikke falder ind under loven, at dette er noget som sker på nettet, og at der er meget lidt som kan gøres. Dette er selvfølgelig totalt urigtigt. Spredning af seksuelle billeder på nettet eller andre it-medier uden samtykke fra den afbildede person er selvfølgelig en overtrædelse af vedkommende persons privatliv, den er egnet til at krænke hans ære og er endvidere krænkelse af kønsfriheden og vedkommendes selvbestemmelsesret. Denne type overtrædelser er ikke noget nyt under solen, seksuelle illustrationer har fulgt menneskeheden helt siden ur-mennesket gjorde gennembrud i teknikken og huggede billeder i sten.[4] Man kan derfor vistnok sige at ordet digital er overflødigt i begrebet digital sexkrænkelse. Her er dette bare et nyt forestillingsbillede af sexkrænkelse, men selve handlingen er fra en ældre tidsalder. Heldigvis

[2] Inger Marie Sunde. A new thing under the Sun? Crime in the Digitized Society. I NSfK´s 58. Research seminar report, 2016, s. 61.
[3] Samme kilde.
[4] Hilaire Barnett: Introduction to Feminist Jurisprudence, 1998, s. 281.

har den store diskussion i de seneste halvår omkring sexkrænkelser bidraget til at disse sager tages mere alvorligt og med et fastere tag, fordi de fleste kan indse hvor alvorlige disse overtrædelser er.

Lovgivningen i de nordiske lande er udformet for at kunne få ram på disse forbrydelser på en eller anden måde. Det ser ud til at hovedvægten har været på krænkelsen af privatlivet og ærekrænkelsesmomentet.[5] Det kan nævnes at den danske regering har i februar 2017 fremlagt en handlingsplan for at styrke indsatsen mod deling af intime billeder og videoer uden samtykke og den mere organiserede udnyttelse af private nøgenbilleder.[6] Den islandske straffelovgivning herom er sådan beskaffen at overtrædelserne om privatlivets fred og ærekrænkelser er underkastet privat påtale, medmindre det drejer sig om nære relationer. Endviderde findes handlingen at være blufærdighedskrænkelse ifølge straffelovens § 209. [7] Islands Højesteret har idømt en mand betinget fængselsstraf for blufærdighedskrænkelse over for sin eks-kæreste ved at offentliggøre billeder af hendes kønsdele på Facebook efter samlivsophør. Det spillede ingen rolle at pigen havde selv taget billederne og sendt dem til manden medens de var par.[8]

3. Politiets beføjelser til indgriben

Politiets beføjelser til at gribe ind har ifølge sagens natur ændret sig en hel del i løbet af de seneste år og årtier. Dette skyldes blandt andet at der er opstået nye typer kriminalitet og nye scenarier af overtrædelser, men dette kan også henføres til krav om styrkere indsats mod terrorhandlinger og organiseret kriminalitet, for blot at nævne nogle eksempler. Selv om det findes nødvendigt at politiet udrustes med beføjelser til at efterforske alvorlig kriminalitet og at deres muligheder udvides for at kunne anvende tvangsmidler, må der dog til stadighed findes vurdering af hvad der findes rimeligt hvor vidt det kan gå, fordi selvfølgelig er politiets tvangsforanstaltninger i strid med borgernes grundlæggende rettigheder. Det er et kendetegn ved disse indgreb at de kan gennemføres med magtanvendelse og de indskrænker borgernes

[5] Se § 264 d i den danske straffelov; kap. 24 i den finske straffelov; § 390 i den norske straffelov og kap. 5 i den svenske straffelov.
[6] https://www.regeringen.dk/nyheder/digitale-kraenkelser/ Gennemset 9. februar 2017.
[7] Bestemmelsen er sålydende: Den som ved uterligt forhold krænker blufærdigheden eller giver offentlig forargelse, straffes med fænbgsel indtil 4 år eller under formildende omstændigheder med fængsel indtil 6 måneder eller bøde under formikldende omstændigheder.
[8] Højesteretsdom 10. december 2015 (nr. 312/2015).

rettigheder, så som privatlivets fred, rejsefriheden, m.v.[9] Der må være en balance mellem politiets beføjelser på den ene side til at efterforske overtrædelser som angår borgernes vægtige samfundsinteresser, sådan som deres sikkerhed, og på den anden side deres rettigheder, sådan som f. eks. deres ret til privatliv. [10] Der er sket en betydelig ændring i de seneste år og endda seneste årtier i de nordiske landes strafferetsplejelovgivning om politiets tvangsindgreb. Delvis kan de henføres til at være følge af terrorangrebene i USA den 11. september 2001 og andre sådanne efterfølgende angreb.[11] Ikke mindst skyldes dette alle de mulige slags og stadige ændringer samt hen raske udvikling af computere og it-udstyr som bliver brugt til at begår kriminalitet.

I Island trådte en ny straffeproceslov nr. 88/2008 i kraft den 1. januar 2009. De vigtigste ændringer i denne nye lov var at det blev nærmere defineret hvilke betingelser måtte være opfyldt for at de enkelte indgreb kan anvendes, som indebærer indskrænkning af menneskerettighederne hos den person som de er rettet mod. I bemærkninger til lovforslaget blev fremhævet:

> *Formålet er først og fremmest at gøre politiets beføjelser til at anvende disse indgreb klarere og at de betinges yderligere ifølge loven, således at borgernes rettigheder ikke bliver indskrænket ud over det højst nødvendige i politiets stræben efter at opklare kriminalitet. Ligeledes er loven udformet på en sådan måde at politiet får hjemmel til anvende metoder som er mest resultatgivende for politiet i dets vigtige rolle at bekæmpe kriminalitet.*[12]

Efter at loven trådte i kraft fremkom der en del kritik, især om telefonaflytninger, som gik ud på at beføjelsen var for åben og at betingelserne for anvendelse af telefonaflytning var uklare, forsvareres adgang til optagne telefonsamtaler var næsten ingen og at reglerne om forbud mod at aflytte samtaler med forsvarere samt destruering af samtaler ikke var i orden.[13] Det har også været kritiseret at kontrollen med gennemførelsen af telefonaflytning ikke har været tilstrækkelig. For at imødekomme denne kritik blev der foretaget ændringer af straffeproceslovens bestemmelser om telefonaflytning ved lov nr. 103/2016 som trådte i kraft den 1. januar 2017. I de generelle bemærkninger i lovforslaget blev følgende fremført:

---

[9] Eiríkur Tómasson. Strafferetsplejen. Efterforskning. Tvangsforanstaltninger, 2012, s. 148.
[10] Se f. eks. Eva Smith. Straffeproces. Grundlæggende regler og principper, 2014, s. 12-14.
[11] Samme kilde, s. 14-15.
[12] Althingsdokument. 252, 135. lovgivende forsamling 2007-2008, s. 117
[13] Se bl.a. Reimar Pétursson. Telefonaflytninger. Advokatbladet, 3. hæfte. 2015, s. 20.

> *Med lovforslaget foreslås at betingelserne for at kunne anvende de indgreb som er nævnt i lovens §§ 81 og 82, stk. 2 i straffeprocesloven bliver skærpet, og at de samtidig gøre mere tydelige. Det foreslås også at der beskikkes en advokat for at varetage den persons interesser som indgrebet er rettet mod, inden retten afsiger kendelse om dette, og i tillæg er fastsat udførlige regler om gennemførelsen af indgreb af denne art og om behandlingen af de oplysninger som er tilvejebragt på denne måde, herunder er det fremhævet at rigsadvokaten skal være den kontrollerende myndighed med at de oplysninger som tilvejebringes ved telefonaflytninger eller lignende indgreb bliver destrueret i overensstemmelse med loven.*[14]

I forbindelse med denne gennemgang kan det nævnes at i sager som blev kaldt for *kraksager,* det vil sige straffesager som opstod på grund af krakket hos de islandske banker i 2008, blev der ført en hård kamp om telefonaflytninger. Fremgangsmåden ved telefonaflytninger i Island var følgende: Efter at kendelse var blevet afsagt om at aflytning kunne foretages, tog cybercrime-efterforskningsenheden hos politiet i hovedstadsområden kontakt med det pågældende teleselskab, som så sørgede for den fornødne kobling til det telefonnummer som skulle aflyttes. Efter tilkoblingen overføres alle telefonsamtaler fra den aflyttede telefon ind på et bestemt system hos politiet hvor de lagres på lydfiler. Oplysninger om de telefonnumre som den pågældende tager kontakt med, kommer ikke med, undtagen fra et teleselskab, og i de tilfælde sker det først nogle minutter efter at samtalen er begyndt, og det er kun numre fra mobiltelefoner som fremkommer. Der kan kun aflyttes i realtid i efterforskningsenhedens lokale hvilket sjældent bliver gjort. Så snart som samtalerne er afsluttet bliver de gjort tilfængelige for efterforskerne. Da den særlige anklagers embede efterforskede straffesager som var knyttet til bankkrakket, kunne det forekomme at sigtedes samtaler med deres forsvarere var blevet optaget på denne måde, d.v.s. var kommet ind på lydfiler. Når efterforskerne blev klare over dette blev disse samtaler destrueret. I Islands Højesterets dom af 1. februar 2016 i sag nr. 842/2014 findes følgende påstand:

> *Det foreligger at tiltaltes samtaler med deres forsvarere blev aflyttet under sagens efterforskning uden at disse optagelser omgående blev destrueret, sådan som det er foreskrevet i § 85, stk. 1 i straffeprocesloven. Disse optagelser er ikke blevet fremlagt, hvilket også er forbudt i henhold til § 134, stk. 4 i loven.*[15]

[14] Althingsdoukument.1087, 145. lovgivende forsamling 2015-2016, s. 2-3.
[15] Højesteretsdom. 1. februar 2016 (842/2014).

Om dette forelå ikke andet end af efterforskerne havde for retten beskrevet hvordan telefonaflytningerne blev gennemført og at når det blev klart at sigtede talte med sin forsvarer blev aflytningen afbrudt. På grund af fejltagelse var denne optagelse ikke blevet tilintetgjort snarest muligt. I denne dom i Højesteret findes også et andet interssant punkt som bør nævnes. I dommen er fremhævet at blandt sagens materiale er:

> *[...] optagelser af telefonsamtaler og anden kommunikation som de tiltalte havde med andre kort tid efter at de havde afgivet forklaring hos politiet, hvor de havde retslig stilling som sigtede, var de ikke forpligtet til at besvare de spørgsmål som de fik stillet angåede de strafbare forhold som de var sigtet for. Ved at aflytte tiltaltes telefoner under disse omstændigheder, til trods for at det var ifølge retskendelser, blev deres ret til retfærdig rettergang krænket ifølge § 70, stk. 1 i grundloven og § 6, stk. i Den Europæiske konvention til beskyttelse af menneskerettigheder og andre grundlæggende frihedsrettigheder jf. lov nr. 62/1994. Disse optagelser vil blive forbiset ved afgørelsen af sagen .*

Det er klart at disse telefonaflytninger blev udført på grundlag af retskendelse og det var ligeledes klart da disse kendelser blev afsagt, at det forventedes at de sigtedes telefoner ville blive aflyttet, og det var også klart at dette drejede sig om et forhold som havde fundet sted lang tid forinden eller før bankkrakket.[16] Dommen fremkaldte en række spørgsmål. Siger Højesteret at telefoner aldrig kan aflyttes hos personer som har fået stilling som sigtede på en formelig måde? Siges herved at der ikke kan foretages aflytninger af telefoner hos personer som har givet forklaring hos politiet som sigtede? I dommen siges at sigtedes telefoner var blevet aflyttet *kort tid* efter at de havde givet forklaring hos politiet. Betyder dette at de sigtedes telefoner kan aflyttes senere og i så fald, hvor lang tid må der været gået? I henhold til en uformel spørgerunde hos anklagemyndighedens repræsentanter i de øvrige nordiske lande, kom de svar at domstolene i deres lande ville næppe været kommet til samme resultat som Islands Højesteret om dette punkt. I Norge kom det forhold til prøve hvorvidt aflytning af telefon hos en person som havde fået stilling som sigtet var i strid med retten til ikke at inkriminere sig ifølge § 6 i Den Europæiske Menneskeretighedskonvention. Norges Højesterets resultat var at det ikke var tilfældet.[17]

[16] Højesteret havde ikke fået disse sager til behandling på dette tidspunkt, fordi på dette tidspunkt forudsatte loven ikke at der skulle beskikkes en advokat for at varetage sigtedes interesser i sager som disse. Dette er senere blevet ændret med lov nr. 103/2016.
[17] Se Avgjörelse fra Höyesteretts kjæremålsutvalg Rt. 20505-205 – KK-2003-2.

I Danmark har der været foretaget en del ændringer af retsplejeloven, blandt andet på baggrund af trusselen om terrorhandlinger, blandt andet i de såkaldte terrorpakker fra årene 2002 og 2006. Retsplejeloven i Norge blev ændret i året 2016. Formålet med lovændringerne var at øge politiets indgrebsmuligheder til at anvende (skjulte tvangsmidler) for at efterforske, afværge og bekæmpe alvorlig kriminalitet.[18] I Sverige trådte i kraft den 1. januar 2015 en lovændring som forankrede anvendelse af tvangsmidler til efterforskning af alvorlige overtrædelser.[19] I Finland gælder bestemmelser i Tvångsmedelslag 22.7.2011/806.[20]

Efterforskning af omfattende og alvorlige overtrædelser sådan som terrorhandlinger og organiseret kriminalitet strækker sig ofte til flere lande og endda verdensdele. Den tekniske udvikling har gjort det muligt at det er nemt at begå kriminalitet på tværs af landegrænser. Gerningsmanden kan sidde hvor som helst i verden ved en computer med internetforbindelse og svindle sig til penge fra personer og virksomheder. Terrororganisationer kan dirigere en udsending til et sted hvor som helst i verden for at begå terrorhandlinger og såvel narkotika som menneskehandelsslaver bliver sendt fra det ene land til det andet. Det bliver stadigt mere vigtigt at politimyndighederne i verden har et godt samarbejde, både når det gælder de mest komplekse og alvorligste forbrydelser, og også når det drejer sig om samarbejde omkring anden kriminalitet, s.s. sexovertrædelser, voldsforbrydelser, økonomiske forbrydelser, o.s.v. Europarådets konvention om IT-kriminalitet (Convention on Cybercrime) som blev vedtaget den 23. november 2001 er meget vigtig når det gælder samarbejde mellem medlemslandene på dette område. I fortsættelse af gennemgangen ovenfor kan det nævnes at konventionens gyldighedsområde er meget udstrakt og begrebet *cybercrime* bør fortolkes med udvidende fortolkning, fordi konventionen finder anvendelse på kriminalitet som er rettet mod elektroniske data og deres fortrolighed, kriminalitet som på nogen måde er relateret til computere og krænkelser på ophavsrettens område.

Konventionen har som mål at der opnås større ensartethed mellem landene når det gælder straffelovgivningen på cybercrime området og at der føres en fælles kriminalpolitik når det gælder indgreb og metoder til efterforskning af sådan kriminalitet samt velfungerende

[18] https://www.regjeringen.no/no/tema/lov-og-rett/kriminalitet-og-politi/innsikt/politimetoder/id2501905/.
[19] https://riksdagen.se/sv/dokument-lagar/arende/betankande/hemliga-tvangsmedel-mot-allvarliga-brott_H201JuU2.
[20] http://www.finlex.fi/sv/laki/ajantasa/2011/20110806.

internationalt samarbejde. Det fremgår af konventionens præambel at blandt målene med den er at:

> *[...] at gøre efterforskning og sagsbehandling af straffelovsovertrædelser som relaterer til edb-systemer og elektroniske data mere effektiv og gør det muligt at tilvejebringe bevismidler i digital form som er knyttet til straffelovsovertrædelser.*[21]

Det kan siges at konventionens overordnede mål er at:

> *For det første at harmonisere substansen i national straffelovgivning og relateret lovgivning med national lovgivning om cybercrime, for det andet at indføre nødvendige straffeprocessuelle bestemmelser for at kunne efterforske og strafforfølge personer som begår kriminalitet ved brug af computersystemer eller digitalt udstyr og for det tredje at fremme øget, hurtigt og velfungerende internationalt samarbejde på dette område.*[22]

Konventionens bestemmelser som handler om at fremme internationalt samarbejde på cybercrime området er selvfølgelig meget vigtige. Navnlig når det haves i tankerne at definitionen af overtrædelserne er så udvidede sådan som tidligere er forklaret, og også når der ses hen til hvor stor del af kriminaliteten i dag har ofte relationer til andre lande.

4. Udfordringer ved efterforskning af straffesager i den digitale verden

Sådan som det er blevet fremhævet flere gange så findes der i langt de fleste tilfælde nogen slags relationer til internettet eller computere når kriminalitet efterforskes. Lad os se på et eksempel om sexkrænkelse. Når det drejer sig om efterforskning af voldtægt kan det være af betydning at undersøge interaktionen mellem den sigtede og offeret, blandt andet på de sociale medier, både inden hændelsen, hvis de kendte hinanden i forvejen, og også efter hændelsen. I sager som handler om grooming af teenagere er det åbenlyst at kommunikationen mellem gerningsmanden og offeret må undersøges, og det kan være af stor betydning at kunne lokalisere offeret i nærheden af sigtedes hjem på et tidspunkt som det

[21] Præambel. Europarådets konvention om IT-kriminalitet, ETS No. 185.
[22] Altingsdokument.905, 132. lovgivende forsamling, 2005-2006, s. 3.

formodede overgreb fandt sted, hvis sigtede nægter at have truffet offeret. Dette punkt var af værdifuld betydning, sammen med andet bevismateriale selvfølgelig, i en sag i Islands Højesteret, nr. 170/2015 af 1. oktober 2015. Tiltalte blev sigtet for at have i to tilfælde krænket en 14 årig pige sexuelt i hans hjem. Den første gang var det for at have øvet sexchickane men den anden gang var det for at have haft samleje med hende uden hendes samtykke, ved ulovlig tvang. Tiltalte erkendte at han havde kommunikeret med pigen via de sociale medier og med sms men han sagde at hun aldrig var kommet i hans hjem. Blandt det som blev lagt til grund da han blev fundet skyldig var telefoniske oplysninger fra pigens telefon som viste at transmission fra telefonen var sendt via en telefonsender i nærheden af sigtedes hjem i begge tilfældene som hun forklarede at hun havde været hjemme hos ham. Dette styrkede pigens forklaring.[23] Nogle sexkrænkelser er faktisk begået på internettet, f. eks. sager som angår besiddelse af børnemisbrugsbilleder eller som angår andre sexkrænkelser i form af grove seksuelle sms-besked som bliver sendt til offeret. I nogle tilfælde kan det være formålstjenligt hvis efterforskeren har kendskab til hvordan bevismidler kan tilvejebringes, bl.a. i form af at opspore en gerningsmand. Det er også af betydning at der lægges grænselinjer om hvor langt der kan gås. I en sag fra Islands Højesteret af 27. august 2012 i sag nr. 562/2012 kom det til prøvelse hvor langt politiets beføjelser til indgreb rækkede, men politiet begærede oplysninger fra teleselskaber om alle opringninger og indringninger via transmissionsanlæg i et bestemt område i et nærmere afgrænset tidsrum. Politiet i Sydlandet havde til efterforskning voldtægt af en pige på et festival på Vestmannaøerne, og det var klart at hverken offeret eller vidner kunne identificere geningsmanden. Da billedmateriale fra overvågningskameraer i området blev undersøgt kunne der derimod ses en mand som passede til offerets og vidners beskrivelse af hans signalement og påklædning, og han sås løbe bort fra området samtidig med at han snakkede i mobiltelefon. Politimesteren nedlagde den påstand for herredsretten at teleselskaber blev forpligtet til at udlevere til politiet oplysninger om alle op- og indringninger igennem transmissionsanlæg i området i et tidsrum af 10 minutters varighed. Herredsretten i Sydlandet tiltrådte kravet, men en teleudbyder kærede kendelsen til Højesteret, som ophævede den. I Højesterettens præmisser blev følgende fremhævet:

> *Ifølge § 80 i straffeprocesloven kan det som led i efterforskningen af en straffesag pålægges teleselskaber at give oplysninger om telefonsamtaler eller anden interaktion i en bestemt telefon, computer eller andet kommunikationsapparat forsåvidt betingelserne som er anført i § 83, stk. 1 og § 84, stk. 1 er opfyldt. Hjemmel til at*

[23] Højesterets dom 1. oktober 2015 (170/2015).

tilvejebringe teleoplysninger ifølge § 80 i straffeproceslovens nr. 88/2008 er et bebyrdende indgreb, og indebærer en undtagelse fra § 70, stk. 1 i grundloven om privatlivets fred, hjemmet og familien. Af denne grund bliver bestemmelsen ikke fortolket mere udvidende end fremgår af dens tekst. Betingelsen for at der gives mulighed for at tilvejebringe det omtalte materiale er at der findes begrundet mistanke om at nogen bestemt telefon eller kommunikationsapparat har været brugt i forbindelse med en strafbar handling. [...] I denne sag sag som er her til afgørelse er sagsøgerens krav ikke rettet mod nogen bestemt telefon eller kommunikationsapparat, men derimod går kravet ud på at der indsamles oplysninger om alle mobiltelefoners op- og indringninger via telesendere som blev opfanget i Herjólfsdalur i et bestemt tidsrum. Eftersom sagsøgers krav er mere vidtgående end der kan rummes indenfor beføjelsen i § 80 i straffeprocesloven nr. 88/2008, bør kravet afslås.[24]

Her mente Højesteret at rettighederne hos en ikke angivet gruppe personer var blevet krænket og at lovens betingelser om at det bør dreje sig om bestemte telefoner eller kommunikationsapparater ikke var opfyldt. I en nylig dom fra Islands Højesteret af 23. februar 2017 i sag nr. 127/2017 blev resultatet noget helt andet. Denne sag var knyttet til politiet i Sydlandets efterforskning af formodet blufærdighedskrænkelse ifølge straffelovens § 209.[25] Politiet havde modtaget nogle anmeldelser i anledning af grove billeder, tekstbesked og videoer fra et bestemt brugernavn på social medie. Politiets mistanke var rettet mod en bestemt person for at stå bag brugernavnet, men personen nægtede at være skyldig. Politimesteren fremlagde krav i herredsretten om at det sociale medies udbyder forpligtedes til at give politiet oplysninger om IP adresse, IMEI serienummer eller andet mærke på det bestemte kommunikationsapparat som relaterede til de omtalte brugerkonto i en bestemt periode. Denne gang afslog herredsretten kravet og henviste bl.a. til Højesterets præmisser i sagen nr. 562/2012:

Politimesterens påstand i sagen er hverken rettet mod en bestemt telefon, computer eller anden slags kommunikationsapparat, eller sigter mod at få oplysninger om telefonsamtaler eller anden kommunikation, men derimod er den rettet mod at få tilbejebragt oplysninger om identificering af et kommunikationsapparat som var koblet til en forbrugerkonto på det sociale medie [...] i et afgrænset tidsrum, men

[24]Højesterets dom 27. august 2012 (562/2012).
[25] Se fodnote 7.

identifikation af et kommunikationsapparat kan hverken antages for at være telefonsamtaler eller anden kommunikation. Der foreligger faktisk intet om hvorvidt der er tale om et eller flere apparater eller hvilken slags apparat dette er. Der foreligger heller intet om hvem er den retmæssige indehaver af den omtalte brugerkonto eller apparat eller apparater. Ifølge ordlyden i straffeproceslovens § 80 findes den ikke at indeholde hjemmel for den tilvejebringelse af oplysninger som sagøgerens påstand er rettet mod. Der findes ikke grundlag for at anvende udvidende fortolkning på lovbestemmelsen ifølge dens ordlyd, bl. a. under henvisning til Islands Højesterets dom.

Politimesteren påkærede kendelsen til Højesteret som kom frem til det modsatte resultat med følgende begrundelse:

Sagsøgers krav går ud på at få oplysninger fra sagsøgte som er teleudbyder, om identifikation af det kommunikationsapparat, som er knyttet til kontoen hos den førnævnte bruger. Her er derfor tale om oplysninger om et bestemt kommunikationsapparat som sagens efterforskning er rettet mod. Omstændighederne i denne sag er forskellige fra sagen i Højesterets dom af 27. august 2012 i sagen nr. 562/2012, hvor der begæredes oplysninger som blev rettet mod et uafgrænset antal brugere af kommunikationsapparater som ikke var på nogen måde indblandet i den sag som var til efterforskning. I medfør af dette findes at sagsøgerens påstand rummes indenfor ordlyden i straffeproceslovens § 80, stk. 1 i belysning af hvordan den fortolkes, hvilket er tidligere blev forklaret.[26]

I disse to sager kan man se en klar forskel efter min mening. På den ene side krav om at få oplysninger om alle mobiltelefoner som blev brugt i et bestemt område i et bestemt tidsrum, og på den anden side at få oplysninger om hvilken kommunikationsapparater er knyttet til et brugernavn som var til efterforskning. Det vil så vise sig hvordan det lykkes at tilvejebringe de ønskede oplysninger fra teleudbyderen, som i dette tilfælde var Facebook.

Der kan nævnes to domme fra Islands Højesteret fra i april 2016, nr. 291/2016 og 297/2016.[27]

[26] Højesterets dom 23. februar 2017 (127/2017)
[27] Højesteretsdomme 20. april 2016 (291/2016 og 297/2016).

Begge sager handler om politiets beslaglæggelse af sigtedes mobiltelefoner som de ikke ville acceptere og gik til retten. Herredsretten tiltrådte kravet om beslaglæggelse i begge tilfælde men kendelserne blev påkæret til Højesteret. Højesteret gav politiet medhold i at de havde været i deres ret til at beslaglægge mobiltelefonerne under henvisning til § 68 i straffeprocesloven uden forudgående kendelse. Politiet havde derimod ikke hjemmel til at undersøge mobiltelefonerne uden kendelse, thi selvom politiet kunne beslaglægge mobiltelefonerne, så forholdt omstændighederne sig således, at de var i substansen kommensurable med de omstændigheder som bestemmelserne i straffeproceslovens § 70, stk. 1 og § 84, stk. 1 omfatter og ifølge analogi er det klart at politiet må have en kendelse for at kunne undersøge indholdet i mobiltelefonen.[28]

Det kan tiltrædes med Højesteret at var rigtigt at opnå kendelse for at politiet kunne undersøge og gennemgranske de sigtedes mobiltelefoner, idet det var ganske simpelt at sikre bevis efter beslaglæggelsen frem til at en kendelse foreligger. Politiet ville på den anden side have haft problemer hvis modbiltelefonen eller andre kommunikationsapparater som skal undersøges, er krypterede. Det sker i voksende grad at sådanne apparater er krypterede og endda på en sådan måde at det er næsten umuligt at trænge ind. Nogle mobiltelefoner er udrustet med fingeraftryksværn, d.v.s at de kan kun åbnes når ejeren trykker med en bestemt finger på en lukketast. Efter min mening ville politiet aldrig have hjemmel til at tvinge en sigtet person til at trykke sin finger på telefonen, men derimod - hvis det var lykkedes politiet at kopiere sigtedes fingeraftryk, som de har hjemmel til at løfte,- mener jeg at de havde hjemmel til at åbne telefonen. Jeg kender dog ikke hvorvidt et sådant forhold har været udsat for retslig prøvelse.

Der kan også spekuleres over et opdigtet eksempel som er relateret til dette. Politiet eftersøger en sigtet mand som er efterlyst og det får oplysninger om at han befinder sig i en bestemt bolig. Når politiet ankommer får politiet tllladelse fra boligejereren til at gå ind i lejligheden

[28] Bestemmelserne er sålydende: § 70, stk. 1 Breve og andre forsendelser som befinder sig hos et post- eller telekommunikationsselskab kan beslaglægges, samt telegrammer, telefaksmeddelselser, e-mailer og anden telekommunikation, som findes i hans varetægt hos et telekommunikationsselskab, for så vidt efterforskningen foretages i forbindelse med en forbrydelse som ifølge loven kan straffes med fængsel. Hvis afsenderen og modtageren ikke er til stede ved beslaglæggelsen, skal de snarest muligt blive oplyst herom, dog sådledes at dette ikke forspilder sagens yderligere efterforskning. Undersøgelse af indholdet af breve, telegrammer og andre forsendelser, som er tilbageholdt ifølge dette stykke, kan kun ske efter en retskendelser. § 84, stk. 1 Beslutning om indgreb efter §§ 80-82 træffes ved kendelse. Dog kan oplysninger efter § 80 gives uden retskendelse hvis der foreligger udtrykkeligt samtykke fra den som råder over telekommunikationen, computeren eller kommunikationsapparatet, eller som er dettes indehaver.

og der anholder det den sigtede mand, som sidder for foran boligejerens computer, men er inde på sin egen Facebook-side. Boligejeren tillader også at boligen ransages. Politiet kan på computerskærmen se at der er åben interaktion mellem den sigtede og et vidne i den sag som er til efterforskning, og at det er klart at denne kommunikation kan være af væsentlig betydning i sagen. Siden på det sociale medie er som sagt åben, og boligejeren har givet tillaldelse til ransagning og beslaglæggelse af computeren, men har politiet tilladelse til at gennemlæse den sigtedes kommunikation uden samtykke fra ham eller ifølge en retskendelse. Spiller det en rolle om politiet kun gennemlæser det som kan ses på skærmen eller kan det også lade interaktionen løbe op og ned på skærmen og læse den i sin helhed? Efter min mening ville det være rigtigst i dette tilfælde at politiet „beslaglægger" Facebook-kontoen, d.v.s. anholder den efterlyste hvis der hjemmel herfor, og eventuelt ændrer passwordet således at den sigtede ikke kan slette kommunikationen, og fremsætte krav i retten om adgang til kontoen i sin helhed og derefter gennemlæse kommunikationen hvis der fås tilladelse til det. Jeg finder ligeledes at politiet kunne fremlægge et foto af skærmen hvor kommunikationen kan ses, til understøttelse af sit krav for retten.

Man må nok erkende at politiets efterforskning i den digitale verden udføres med de hjælpemidler og kundskaber som politiet er i besiddelse af til enhver tid. Det er derfor uhyre vigtigt – sådan som jeg har tidligere nævnt – at politiet får tilstrækkelige resurser til at politifolkene kan vedligeholde deres viden på dette område og lære mere og til køb af nødvendigt og tidssvarende udstyr. Der er også et andet tvivlspørgsmål, nemlig hvor langt politiet må gå i efterforskningsøjemed? Selv om politiet kan tilvejebringe bestemte oplysninger eller data, betyder det så også at de har hjemmel til det? I en dom fra Danmarks Højesteret af 10. maj 2012 (UfR 2012.2614H) blev spørgsmålet om jurisdiktion sat på prøve i en narkosag hvorvidt det danske politi kunne beslaglægge og undersøge indholdet på en Facebook-side hos sigtede og Messenger-delen af hans Facebook –side. Forsvareren hævdede at alle oplysningerne på sigtedes Facebook-profil er lagret på en server i Californien og at Messenger-profilen er hjemmehørende i Luxembourg. Han gjorde gældende at indgreb uden for landets grænser kræver lovhjemmel og tilladelse fra de pågældende lands myndigheder, og disse forelå ikke. Under efterforskningen havde politiet via telefonaflytning fået kendskab til koderne til Facebook- og Messenger-profilerne. Politiet havde foretaget en kortvarig aflæsning af Facebook-profilen med henblik på at konstatere, om der fortsat var adgang til profilen. Danmarks Højesteret fandt frem til det resultat at politiets indgreb har karakter af gentagne hemmelige ransagninger og at betingelserne efter retsplejelovens § 793, stk.1, nr. 1

jf § 799 herfor er opfyldt. Da kriminaliteten var undergivet dansk straffemyndighed, da sagen efterforskes af danske myndigheder, og da indgrebene kan foretages uden at involvere udenlandske myndigheder, var det uden betydning at sigtede i en periode befandt sig i udlandet og at oplysningerne på profilerne befinder sig på servere i udlandet.[29] Efter min opfattelse er denne konklusion hos Danmarks Højesteret rigtig, det spiller en afgørende rolle at danske myndigheder kan komme ind på siderne hos sigtede fra hvilken som helst computer som er tilsluttet internettet og oplysninge som bliver lagret på internettet. Det må ligeledes haves i tankerne at brugere af tjenester hos teleudbyderne af sociale medier, e-mail, m.m. meget sjældent har kendskab til hvor deres data bliver lagret og det kan endda være ganske besværligt for efterforskerne at finde ud af det. Da den såkaldte „Baugs-sag", som var knyttet til en af bankkraksagerne, blev efterforsket fik den særlige anklager hjemmel til ransagning hos et islandsk teleselskab med henblik på at beslaglægge og kopiere data i digital form, som selskabet lagrede for bestemte islandske selskaber. Serveren som lagrede de digitale data, heriblandt e-mails, var i Storbritannien. I forretningsstedet hos det islandske teleselskab kunne man derimod logge sig ind og „suge" data ud. Hvis det pågældende teleselskab havde også været i Storbritannien, havde man selvsagt måttet søge bistand hos myndighederne dér i landet, for at kunne gennemføre søgning og beslaglæggelse på forretningsstedet.

5. Afsluttende bemærkninger

Det er indlysende at der henstår utallige spørgsmål ubesvarede, som er relateret til efterforskning og retsforfølgning i vores tidsalder. Teknikken galoperer og gør store fremskridt og det slider på politiet at følge med i denne udvikling og holde trit med de kriminelle. Jeg finder det nødvendigt at tage et pusterum og overveje hvorvidt og hvilken slags kriminalitet vi skal gruppere som cybercrime og hvornår vi blot ser et nyt forestillingsbillede af kendt kriminalitet. Islands Højesteret fandt for nylig en mand skyldig for forsøg til voldtægt ved at opnå kontakt med en ung dreng igennem Snapchat under falsk navn. Han fik drengen til at deltage i seksuel snak og fik ham til at sende billeder af sine kønsorganer. Den næste dag truede han drengen med billeddeling på det sociale netværk og at lægge ud deres seksuelle chat, hvis drengen ikke havde seksuel omgængelse med ham inden et bestemt tidspunkt om aftenen.[30] I denne sag bestod handlingen simpelthed af forsøg på at

[29] Lars Bo Langsted har fremsat interessante bemærkninger om dommen i Digital Evidence and Electronic Signature Law Review, 10. hæfte. 2013, s. 164-165.
[30] Højesteretsdom 15. december 2016 (441/2016).

opnå seksuel omgængelse igennem ulovlig tvang – forsøg til tvang. Denne forbrydelse er efter min mening ikke nogen særlig cybercrime selv om den sociale medie Snapchat blev andvendt og at al kommunikation foregik dér og på Facebook. Nogle overtrædelser er ganske vist af sådan karakter at de faktisk er cybercrime og det er enormt vigtigt at politiet har oprettet cybercrime efterforskningsenheder som er i stand til at efterforske sådan kriminalitet. Virkeligheden er derimod den at alle som deltager i efterforskning af straffesager, deres retsforfølgning og anden behandling i retshåndhævelsessystemet har basale kundskaber til computersystemer og de vigtigste sociale medier. Det er endvidere klart at myndighedernes samarbejde omkring disse overtrædelser er højt prioriteret og i denne relation er det nære nordiske samarbejde og Europarådet konvention om cybercrime meget vigtige. Politiet og anklagemyndigheden står over for forskellige udfordringer under efterforskning af straffesager i en digital verden, navnlig når det gælder alvorlige forbrydelser sådan som terrorhandlinger og organiseret kriminalitet. Men det er lige så vigtigt at være opmærksomme på behovet for at sikre den rette balance mellem hensynet til retshåndhævelsen og respekten for de grundlæggende menneskerettigheder.