# Jubileumsskrift till Juridiska institutionen 40 år

REDAKTÖRER
ÖRJAN EDSTRÖM, JOHAN LINDHOLM &
RUTH MANNELQVIST

UMEÅ UNIVERSITET

**Juridiska institutionen**
Umeå 2017

ISSN: 1404-9198
ISBN: 978-91-7601-793-7
Ev. info om Omslag/sättning/omslagsbild:
Elektronisk version tillgänglig på http://umu.diva-portal.org/
Tryck/Printed by: UmU Tryckservice, Umeå universitet
Umeå, Sverige 2017

# Näthat som rättslig utmaning i nutid och framtid

THERESE ENARSSON*

## 1 Inledning

Juridiken ställs ständigt inför nya utmaningar i takt med förändringar i samhället. Internet har gett upphov till helt nya möjligheter att kommunicera människor emellan, att dela såväl tankar, åsikter och känslor som information, musik eller filmer. Detta kan vara något mycket positivt, något som leder till att människor når ut, får intryck och sociala relationer, och att de kan delta i samhällsdebatter över hela världen. Internets många möjligheter till kommunikation kan dock även leda till hot eller kränkningar, något som ofta kallas för *näthat*.

Problematiken med näthat har under de senaste åren fått stor uppmärksamhet i samhället, inte minst medialt, och många har vittnat om den utsatthet de i olika sammanhang har upplevt på internet. Näthatet har kretsat kring allt från unga och barn som blir utsatta för mobbning och andra kränkningar på sociala medier, journalister och politiker som hotas och hatas i särskilda forum, till personer som kränks genom att någon utan tillstånd sprider bilder eller filmer av dem, där materialet som sådant eller spridandet av det syftar till att vara kränkande.[1]

Den ökade användningen av ny teknik medför därmed att lagstiftaren ställs inför utmaningar där rätten måste utvecklas på ett sätt som gör att människor kan skyddas från grova påhopp eller stor spridning av kränkningar. Detta måste också ske utan att den rättsliga utvecklingen i alltför stor utsträckning inskränker den nya teknikens ljusare sidor som den ökade möjligheten att uttrycka sig, dela

* Therese Enarsson är lektor och forskar och undervisar bland annat om brottsoffers rättigheter, digital rättsvetenskap samt i ämnena rättshistoria och rättsfilosofi.

[1] Se bl.a. Enarsson, Therese, Utsatthet på nätet: Möjligheter till rättslig upprättelse vid ärekränkningar på internet, *Juridisk Tidskrift*, 2015, nr 4, s. 877–878; Dunkels, Elza, *Nätmobbning, näthat och nätkärlek. Kunskaper och strategier för en bättre vardag på nätet*, Gothia fortbildning AB, Stockholm 2015, s. 27.

och sprida åsikter och tillhandahålla information som ett led i ett demokratiskt samhälle.

Från senhösten 2013 till och med våren 2017 bedrev jag projektet *Offer för näthat. En rättsvetenskaplig studie av brottsoffers möjlighet till upprättelse vid hot och kränkningar på internet*[2] och i projektet analyserades brottsoffers rättsliga förutsättningar till upprättelse, utifrån såväl straffregleringens bakomliggande syften och brottsoffers behov som yttrandefrihetens gränser. Detta antologibidrag syftar till att sammanfattande lyfta fram vissa väsentliga aspekter av den juridiska problematik kring näthat som har aktualiserats under projektets gång[3] och att i ljuset av dessa avslutningsvis diskutera framtida rättsliga utmaningar i fråga om hanteringen av näthat.

## 2 Kontextuella möjligheter, skyldigheter och rättigheter

Den främsta identifierade rättsliga utmaningen på näthatsområdet under projektets gång är dess mycket kontextuella natur. Detta präglar flera av de mest avgörande frågorna för att hantera när enskilda utsätts för hot och kränkningar på internet, som att ett uttalandes straffbarhet kan bero på sammanhanget, att möjligheterna att få tillgång till bevisning kan vara beroende av dels vilket brott det rör sig om dels vilken typ av internetplattform som aktualiserats eller vilken aktör som ansvarar för sidan. Om det föreligger en möjlighet eller ett rättsligt tvång att avlägsna uppgifter beror på såväl vilken typ av uttalande eller uppgift det rör sig om, som vilken aktör och plattform som är aktuell i den enskilda situationen. Denna kontextuella natur kommer på flera sätt bli tydlig i de delfrågor som diskuteras nedan.

### *2.1 Övergripande rättsligt ramverk utifrån Europakonventionen*

Ett övergripande rättsligt ramverk för hur vi i Sverige ska hantera och rättsligt reglera, utreda och lagföra kränkningar mot enskilda ställs upp av Europakonventionen och Europadomstolens praxis. Detta är därför en utgångspunkt för Sveriges möjligheter och skyldigheter att hantera frågan om näthat på ett sätt som säkerställer en balans mellan skyddet för enskilda mot kränkningar av person, ställt mot andra intressen som skyddas under konventionen, som yttrandefrihet. Dessa två intressen skyddas främst genom

[2] Detta antologibidrag tjänar som en avslutande och sammanfattande publikation av projektet som finansierades av Brottsofferfonden.

[3] Projektet pågick mellan åren 2013 och 2017.

artikel 8 och artikel 10. Artikel 8 med sitt skydd för privat- och familjeliv, hem och korrespondens, ger en enskild person, ett offer för näthat exempelvis, ett skydd utifrån konventionen och ålägger, tillsammans med konventionen i sin helhet, staterna en omfattande skyldighet att se till att individers personliga integritet och privatliv skyddas. Artikel 10 ger ett uttryckligt skydd för yttrandefriheten.[4]

Som konventionsstat har Sverige såväl positiva som negativa skyldigheter under konventionen. Det som främst brukar framhållas i förhållande till staternas ansvar under konventionen är de negativa skyldigheterna, det vill säga, skyldigheten för staterna själva att inte kränka någon av de rättigheter som tillskrivs medborgarna under konventionen. De positiva skyldigheterna innebär ett ansvar för staterna att säkerställa att medborgarnas rättigheter även i praktiken skyddas. Det innebär att staterna ska skydda enskilda mot kränkningar från andra medborgare genom någon form av aktiv handling, till exempel kriminalisering av handlingar och möjligheterna att få tillgång till en rättsprocess. Att staterna lever upp till sina positiva skyldigheter kan därför ses som ett processuellt komplement till ett materiellt regelverk, som ska ge ett starkare rättsligt skydd i praktiken.[5]

I förhållande till näthat är det framför allt de positiva skyldigheterna under artikel 8 som aktualiseras då staten ska säkerställa att individer åtnjuter ett skydd för sina rättigheter även när dessa rättigheter kränks av andra enskilda på det horisontella planet. Sverige måste alltså säkerställa att det finns ett skydd mot olika typer av kränkningar mot enskilda. Däremot är det värt att poängtera att det inte finns något specifikt skydd just för kränkningar på internet utifrån konventionen, och att andra artiklar än artikel 8 kan aktualiseras vid bedömningar, inte minst artikel 10, men vad gäller just de positiva skyldigheterna i förhållande till näthat rör det främst skyddet för privatlivet och artikel 8. Området är dock som nämnts präglat av avvägningar, och det rättsliga skydd som staterna uppställer för individens privatliv måste samtidigt balanseras mot de negativa skyldigheter som Sverige har utifrån artikel 10, nämligen att säkerställa att staten inte inskränker enskildas yttrandefrihet på ett oproportionerligt sätt.[6]

[4] Xenos, Dimitris, The Positive Obligations of the State under the European Convention on Human Rights, Routledge, 2012, s. 12–13.

[5] Se bl.a. Enarsson, Therese & Naarttijärvi, Markus, ”Näthat och det positiva ansvaret under Europakonventionen: viktimologiska hänsyn och normativa utgångspunkter”, *Europarättslig tidskrift*, 2015, nr 3, s. 556–576; Xenos, 2012; Mowbray, Alistair, *The Development of Positive Obligations under the European Convention on Human Rights by the European Court of Human Rights*, Hart Publishing, Oxford 2004, s. 2.

[6] Enarsson & Naarttijärvi, 2015, s. 560–563.

I projektet utgick inledningsvis resonemanget från en konflikt mellan dessa två skyddsintressen, det vill säga i de många situationer där brottsoffrets integritet ställs mot förövarens rätt till yttrandefrihet. Denna utgångspunkt problematiserades dock efterhand och vikten av att även kunna se dem som samspelande ökade. Det är nämligen väsentligt att uppmärksamma att inte endast den som yttrar sig kränkande på internet kan ha rätt till värnande om sin yttrandefrihet, utan även offret. Det är av högsta vikt för ett brottsoffer att uppleva att det finns ett skydd när denne har blivit utsatt på internet. Annars finns det en risk att personen drar sig undan och inte vill delta i det offentliga samtalet, att den personen begränsar sig och förlorar tillgång till det digitala samhället.[7] Att upprätthålla detta skydd är givetvis också viktigt även för andra som inte blivit utsatta men som räds det. Att upprätthålla ett skydd för den personliga integriteten, kanske genom att på vissa sätt inskränka yttrandefriheten, kan då samtidigt *gynna* yttrandefriheten genom att bidra till ett internet där människor inte räds att delta. Detta gör att avvägningen mellan dessa två intressen om möjligt blir ännu mer väsentlig ur ett brottsofferperspektiv, då ett starkt och välavvägt skydd inte endast ska säkerställa brottsoffrens möjligheter till en rättslig upprättelse och skydd för sin integritet och person, utan också för brottsoffrets möjligheter att själva våga och kunna uttrycka sig på internet, och därmed i samhället.[8]

Liksom skyddet för yttrandefriheten är skyddet för den personliga integriteten inte ensidigt. Det är inte endast brottsoffrets integritet som måste värnas, utan även den misstänktes, i egenskap av medborgare med rätt till skydd för sin integritet. Det tillgodoses genom skyddsmekanismer för den personliga integriteten som exempelvis rätt till förtrolig kommunikation och skydd för personuppgifter på internet, något som syftar till att skydda allas integritet när de vistas på internet. Detta integritetsskydd är också i förlängningen ägnat att bidra till individens autonomi och självbestämmande något som i slutändan är en förutsättning för den fria åsiktsbildningen. [9]

[7] Keats Citron, Danielle, ”Civil Rights in Our Information Age”, i Levmore, Saul & Nussbaum C., Martha (red), *The Offensive Internet*, s. 31–49, särskilt s. 31.

[8] Detta resonemang utvecklas utförligt i Enarsson Therese & Naarttijärvi, Markus, ”Is it all part of the game?: Victim differentiation and the normative protection of victims of online antagonism under the European Convention on Human Rights”, *International Review of Victimology*, vol. 22, no. 2, 2016 s. 123–138.

[9] Se bland annat Naarttijärvi, Markus, ”Övervakning av metadata som spelplan för rättsliga principkonflikter” i *Övervakning och integritet: Teknik, skydd och aktörer i det nya kontrollandskapet*, Pettersson, Tobbe & Agrell, Wilhelm (red.), Carlsson Bokförlag, Stockholm 2016.

Skyddet för den personliga integriteten påverkar därför hur kriminaliseringar av olika beteenden ska utformas och hanteras samt de utredningsmöjligheter som tillåts, under Europakonventionen, vid misstanke om brott i olika situationer.

## *2.2 Kriminalisering av näthat*

Att i projektet analysera de rättsliga möjligheterna att arbeta mot näthat innebar inledningsvis att identifiera vad näthat, rent juridiskt, kan vara.[10] Det är inte som sådant ett rättsligt begrepp och det kan omfatta en mängd handlingar som kan inrymmas inom befintliga straffbestämmelser. Exempelvis kan näthat utgöra olaga hot[11], ofredande[12] eller olaga förföljelse.[13] En stor mängd av de kränkningar som sker på internet utgörs också av ärekränkningar, det vill säga förolämpningar och förtal samt grovt förtal.[14] Att det senare är brottstyper som har ökat under senare år och att många blir utsatta för just förtal på internet har lett fram till en förändring av BrB 5 kap 5 § som reglerar ärekränkningsbrotten, så att något fler fall av förtal, som i normalfallet är målsägandebrott, ska kunna drivas av åklagare. De allra flesta fall ska dock fortfarande inte drivas av åklagare utan om brottsoffret vill driva frågan får hen göra detta själv genom ett enskilt åtal. Detta är problematiskt, då det kräver resurser, kunskap och kraft att driva en process, inte minst om du har blivit utsatt för ett brott som kan vara mycket kränkande. Men det faktum att fler, om än inte alla, kan få tillgång till en straffrättslig process driven av en åklagare får ändå ses som positivt ur ett brottsofferperspektiv.[15]

Ändringen genomfördes framför allt på grund av framväxten och utvecklingen av internet och den ökade spridningsrisk som detta medför för den

[10] För ett mer utvecklat resonemang kring detta, se Enarsson & Naarttijärvi, 2015; Enarsson, 2014.

[11] Brottsbalk, BrB, (1962:700) 4 kap. 5. Se bl.a. Hovrätten för västra Sverige 2017-02-20 (mål nr B 1050-17) om olaga hot via bland annat Snapchat; Svea Hovrätt 2012-07-02 (mål nr B 4235-12) om olaga hot på Facebook.

[12] BrB 4 kap. 7. Se bl.a. Svea Hovrätt dom 2017-04-11(mål nr B 9546-16) om bl.a. ofredande genom textmeddelanden; Göta Hovrätts dom 2012-11-07 (mål nr B 81-12) om ofredande och förtal på Facebook.

[13] BrB 4 kap. 4b §. Se Göta Hovrätt 2015-01-21 (mål nr B 2663-14) om olaga förföljelse, bl.a via en mycket stor mängd e-postmeddelanden.

[14] Brottsförebyggande rådet (BRÅ), *Polisanmälda hot och kränkningar mot enskilda personer via internet*, Rapport 2015:6, 2015; Svensson, Måns & Dahlstrand, Karl, *Kränkningar, trakasserier och hot på nätet, Delrapport till Ungdomsstyrelsen med fokus på kvantitativ kartläggning*, Lunds universitet, 2013, s. 5.

[15] Enarsson, 2014, s. 880–882.

som utsätts för exempelvis förtal. Lagstiftningen tar också särskilt sikte på att det i vissa situationer kan vara speciellt svårt för den som utsatts att själv kunna driva en process, som när den drabbade är ung.[16]

Detta är ytterligare ett exempel på det kontextberoende skyddet vid näthat. Att olika grupper kan ha olika skydd och möjligheter när de utsatts för näthat, är också något som kan utläsas av Europakonventionen utifrån Europadomstolens praxis. Konventionen ställer krav på särskilt starkt skydd för vissa grupper av offer, och i projektet har det konstaterats att skyddet som staterna ska tillförsäkra olika grupper beror på i vilket sammanhang olika uttalanden görs och mot vem. Vissa grupper har ett särskilt starkt skydd, exempelvis utifrån att de är barn eller att de utsätts på grund av sin hudfärg eller religion. Kan brottet anses utgöra så kallat *hate speech*, alltså kränkningar riktade mot exempelvis någons hudfärg eller religion, behöver inte dessa uttalanden vägas mot artikel 10 på samma sätt som andra typer av kränkningar. Sådana uttalanden skyddas nämligen inte under konventionen, utifrån undantaget i artikel 17 som stadgar att varken stater eller individer får stödja sig på konventionen för att utplåna eller oproportionerligt inskränka det som skyddas under den.

Om uttalanden riktas mot andra grupper, som politiker, kan dessa brottsoffer däremot ha ett svagare skydd, då det har bedömts som olämpligt, ibland rent av felaktigt, att uttalanden som kan ses som en del i en politisk diskussion eller en öppen debatt ska kunna leda till en rättsprocess i ljuset av yttrandefriheten.[17] Yttrandefrihetens utgångspunkt är nämligen att skydda alla typer av yttringar i alla former – ljud, bild, film – för att säkerställa allt från människors rätt att uttrycka sig genom konst till möjligheten att granska politik eller avslöja korruption. Detta medför att eventuella inskränkningar måste vägas mot till exempel möjligheterna till en öppen politisk debatt. Det kan i praktiken medföra att politiker får ett något sämre skydd mot näthat, då taket för vad som ska få säga är högre i sådana sammanhang.[18] Uttalandets karaktär spelar därför också roll, oavsett vem den utsatta är, och alltså inte bara vem offret är eller i vilken

[16] Prop. 2013/14:47 Några ändringar på tryck- och yttrandefrihetens område, s. 25; Åklagarmyndigheten, RättsPM 2014:2, Förtal och förolämpning, s. 19.

[17] Se bl.a. Rainey, Bernadette, m.fl., *Jacobs, White & Ovey: The European Convention on Human Rights*, uppl. 6, Oxford University Press, Oxford 2014, s. 438; Grabenwarter, Christof, *European Convention on Human Rights – Commentary*, Verlag C.H. Beck oHJ, München 2014, s. 266.

[18] Se bl.a. Handyside mot Förenade Konungariket, (5493/72) Europadomstolens dom (GC) den 7 december 1976, § 49; Enarsson, Therese, ”Näthatets offer: utsatthet och upprättelse”, i Granström, Görel & Mannelqvist, Ruth (red.) *Brottsoffer: rättsliga perspektiv*, Studentlitteratur AB, Lund, 2016 s. 79–92, särskilt s. 83.

egenskap hen blir utsatt. I de fall uttalandena tar sikte på de mest privata aspekterna av en persons liv, till exempel sexuallivet, och därmed är särskilt integritetskränkande, ska också de offren ha ett starkare skydd.[19]

Det ovanstående innebär en möjlighet vid utformandet av lagstiftning som skyddar offer för näthat, då det skapar ett utrymme att i lagstiftningen ta särskild hänsyn till vissa identifierade skyddsvärda grupper och vissa mindre skyddsvärda uttalanden. När exempelvis Sverige ska säkerställa ett skydd för de som utsätts för näthat kan detta vara en utgångspunkt för översyn och utveckling av lagstiftning som syftar till att skydda mot näthat. Att i den lagstiftningsprocessen särskilt beakta dessa identifierade skyddsvärda grupper, som barn, offer för hatbrott eller offer för särskilt integritetskränkande brott är därför ett sätt att bibehålla eller skapa rättsliga vägar till upprättelse vid utsatthet för näthat, utan att riskera konflikter med yttrandefriheten utifrån konventionen.[20] I projektet har det därför kunnat visas att det i många fall finns rättsliga förutsättningar till upprättelse vid utsatthet för näthat, att många handlingar är kriminaliserade, men att brottets natur kommer att påverka vilka rättsliga lösningar som främst aktualiserats. Det påverkar i sin tur vilken möjlighet det finns för brottsoffret att polis och åklagare utreder och driver ärendet.

Som nämnts är det inte bara kriminalisering av kränkningar som är väsentligt vid rättslig hantering av näthat, utan också möjligheterna att faktiskt utreda brotten. En kriminalisering som sådan, som sedan inte kan åtföljas av lämpliga utredningsåtgärder, riskerar att ge en begränsad avskräckande effekt.[21] Det i sin tur kan bidra till ytterligare förväntningar från brottsoffrets sida som myndigheterna får svårt att leva upp till, vilket då riskerar att påverka förtroendet för rättsvårdande myndigheter negativt. Därför måste det finnas faktiska möjligheter att utreda, och därmed, lagföra brotten.

## *2.3 Möjligheter att utreda kränkningar på internet*

En förutsättning för att någon ska kunna lagföras för att ha kränkt eller hotat någon på internet är att den personen går att identifiera. I vissa fall är detta enkelt, då personen antingen erkänt att denna gjort vissa uttalanden (men kanske inte

[19] Se bl.a. K.U. mot Finland, (2872/02), Europadomstolens dom den 2 december 2008, §§ 6–14; Jersild mot Danmark (15890/89), Europadomstolens dom (GC) den 23 September 1994, § 30; Gündüz mot Turkiet (35071/97), Europadomstolens dom den 4 december 2003, §§ 40–41; Enarsson & Naarttijärvi, 2016, bl.a. s. 132–135.

[20] Detta resonemang utvecklas i Enarsson & Naarttijärvi, 2016.

[21] K.U. mot Finland, § 46.

håller med om de är straffbarhet) eller då tydliga identifierande uppgifter finns tillgängliga, exempelvis om någon använt sin telefon och ett telefonnummer som leder tillbaka till den personen. Det finns dock situationer där personen valt att dölja sin identitet. Om gärningen begåtts på etablerade sociala medier exempelvis, finns ofta information som går att härleda tillbaka till en person, som ett IP-nummer. Brottsbekämpande myndigheter är dock i stor utsträckning beroende av upprättade samarbeten med sociala medieplattformar, inte minst när näthatet sker på internetsidor som är etablerade utomlands. Rikspolisstyrelsen har i detta sammanhang upprättat ett samarbete med Facebook som innebär att det vid Rikspolisstyrelsens IT-sektion finns en central funktion som har direktkontakt med Facebook och kan utgöra ett stöd för andra utredande polisenheter med kontakter och förfrågningar gentemot företaget.[22] Genom denna funktion kan polisen ofta få tillgång till ett IP-nummer, och det går i regel relativt snabbt.[23] För att sedan få tillgång till vem som står bakom det aktuella IP-numret sker direktkontakter från polis eller åklagare till aktuell internet- eller mobiloperatör. Då sådan information är sekretessbelagd krävs det dock misstanke om brott för att utlämning ska få ske.[24] Innan år 2012 krävdes det också fängelse i straffskalan för att kunna begära ut sådana uppgifter, men i ljuset av ökningen av just ärekränkningar på internet ändrades det.[25]

Detta är ett snabbare och mer effektivt sätt att kunna utreda kränkningar på internet, jämfört med att behöva begära rättshjälp från andra länder. Att begära rättshjälp, alltså rättslig hjälp från brottsbekämpande myndigheter och domstolar utomlands, blir dock aktuellt om polisen vill få ut uppgifter som går utöver de identifikationsuppgifter, till exempel bilder eller annat innehåll från någons konto. Möjligheterna att framgångsrikt begära rättshjälp beror dock i stor utsträckning på vilket brott som misstänkts – om endast böter finns i straffskalan anses det exempelvis inte resursmässigt försvarbart att begära rättshjälp – samt i vilket land som den aktuella bloggen, hemsidan eller liknande har sin hemvist.

[22] Rikspolisstyrelsen, ”Polisen och Facebook i samarbete mot näthat”, tillgänglig på *www.polisen.se*, 27 oktober 2014. Se även Niklasson, Anette, ”Polis och Facebook mot näthat”, i *Sydsvenskan* den 31 oktober 2014.

[23] I september år 2014 hade exempelvis 512 förfrågningar om begäran av uppgifter gjorts av Polisen och i 501 av fallen, se Rikspolisstyrelsen, ”Polisen och Facebook i samarbete mot näthat”, tillgänglig på *www.polisen.se* 27 oktober 2014. Se även Niklasson, 2014; Enarsson, 2014, s. 885.

[24] Lag (2003:389) om elektronisk kommunikation 6 kap. 20 §.

[25] Prop. 2011/12:55 De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation.

Detta har sin grund i att möjligheterna till rättshjälp är beroende av upprättade avtal och konventioner stater emellan.[26] Detta påverkar möjligheterna att framgångsrikt och i rimlig tid utreda olika former av näthat mot brottsoffer i Sverige. Värt att poängtera är dock att lagförslag, som presenterades under senvåren 2017, för att implementera EU:s direktiv om en europeisk utredningsorder. Förslaget innebär att domstol eller åklagare i Sverige ska kunna utfärda en europeisk utredningsorder för erkännande och verkställighet i en annan medlemsstat, om det finns bevisning för ett brott som utreds i Sverige. Detta skulle kunna effektivisera utredningen av vissa former av näthat, i vart fall vid grövre brott.[27]

I projektet har det också kunnat visas att utredningsmöjligheterna till stor del är beroende av hur brottet rubriceras under förundersökningens gång. Om brottet har fängelse i straffskalan, som exempelvis olaga hot, finns möjligheter till fler straffprocessuella tvångsmedel, som husrannsakan för att beslagta någons dator eller kroppsvisitation för att exempelvis få tillgång till någons mobiltelefon, än om brottet endast har böter i straffskalan, vilket är fallet vid rubriceringen förtal. Vid förtal kan det vara möjligt med beslag, om det anses proportionerligt, för att exempelvis ta någons telefon. Då det däremot inte är aktuellt med kroppsvisitation eller husrannsakan skulle det dock förutsätta att telefonen frivilligt överlåts eller är framtagen i ett möte med polisen. [28] I de fall där straffprocessuella tvångsmedel kan användas ökar givetvis möjligheterna att utreda och frambringa bevisning i skuldfrågan vid näthat.

Det bör dock samtidigt framhållas att möjligheter för brottsbekämpande myndigheter att få tillgång till olika typer av identifierande uppgifter rörande människor som kan misstänkas för brott är en inskränkning av deras skydd för den personliga integriteten, varför det måste finnas en proportionalitet i de rättsliga möjligheterna till inhämtning. Att finna en sådan balans är dock inte utan svårigheter, och det har aktualiserats inte minst i frågan om datalagring, alltså krav på operatörer att under viss tid spara identifierande uppgifter om användare, som IP-nummer. Tidigare gällde i svensk lagstiftning att uppgifter skulle lagras i

[26] Se t.ex. internationell rättshjälp genom lag (2000:562) om internationell rättslig hjälp i brottmål; EU:s konvention om ömsesidig rättslig hjälp i brottmål mellan EU:s medlemsstater (2000 års EU-konvention); Avtal med Amerikas förenta stater om ömsesidig rättslig hjälp i brottmål.

[27] Bestämmelserna föreslås träda i kraft den 1 december 2017. Se Lagrådsremiss Nya regler om bevisinhämtning inom EU, 1 juni 2017.

[28] Rättegångsbalk (1942:740) 27 kap. 1 § st. 2.

sex månader, för att sedan raderas, utifrån det så kallade datalagringsdirektivet.[29] Direktivet har dock ogiltigförklarats av EU-domstolen och får inte tillämpas, då insamlandet av uppgifter på den tidigare nivån inte har ansetts vara tillräckligt proportionerligt eller rättssäkert, och innebär ett alltför stort ingrepp i människors privatliv. Detta medför att ett raderingskrav istället föreligger, och operatörer är skyldiga att radera uppgifterna så snart de inte längre behövs för deras verksamheter, exempelvis för fakturering.[30] Brottsbekämpande myndigheter kan då endast få tillgång till uppgifter om de faktiskt och utifrån operatörens behov finns lagrade, vilket är ytterligare en försvårande faktor i utredandet av näthat. För svensk del utreds frågan om hanteringen av datalagring för närvarande och ska delredovisas under hösten 2017.[31] Frågan visar på ytterligare nödvändiga avvägningar vad gäller å ena sidan skyldigheten för Sverige att tillhandahålla effektiva rättsliga medel för brottsbekämpande myndigheter, och å andra sidan skyldigheten att värna om den personliga integriteten på internet.

## *2.4 Avlägsnande av material*

För att studera frågan om möjligheter till upprättelse för de som utsätts för näthat kom projektet inte endast att omfatta frågor om kriminalisering och möjligheter till utredning av sådana gärningar, utan också möjligheter till avlägsnande av uppgifter, då detta kan vara en viktig faktor för brottsoffer. Det som har studerats är vissa specifika situationer, där andra aktörer än den som först publicerat inlägget eller informationen kan ha en skyldighet att avlägsna den. Detta så kallade *tredjepartsansvar*, innebär ett ansvar att avlägsna eller *inte* avlägsna innehåll producerat av andra på en sida under ens ansvar. Det ansvaret är väsentligt för att studera vilka möjligheter det kan finnas för brottsoffer att undvika och minska spridning av material som denna inte vill ska finnas tillgängligt på internet. Detta

[29] Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG.

[30] Förenade målen C-293/12 och C-594/12, Digital Rights Ireland och Seitlinger m.fl., Domstolens dom (stora avdelningen) av den 8 april 2014; förenade målen C-203/15 och C-698/15, Tele2 Sverige AB mot Post- och telestyrelsen och Secretary of State for the Home Department mot Watson m.fl., Domstolens dom (stora avdelningen) av den 21 december 2016.

[31] Dir. 2017:16 Datalagring och EU-rätten. Uppdraget i sin helhet ska redovisas senast i augusti 2018.

är särskilt viktigt då det inte i alla situationer kommer gå att utreda vem som laddat upp ett visst material och få den personen lagförd. Dessutom är det ibland svårt, för att inte säga omöjligt, att helt förutse den spridning som ett visst material får, varför det kanske inte heller går att helt avlägsna eller stoppa spridning av ett visst material ens för gärningspersonen själv, även om den personen så skulle vilja.[32]

Möjligheterna att kunna kräva att uppgifter avlägsnas visade sig dock i mycket stor utsträckning beroende av vilken typ av uttalande eller annat material som den utsatta vill ha avlägsnat och var det har publicerats. En fråga som har kommit att aktualiseras mycket under senare år är det hat som sprids i kommentarsfält till nyhetsartiklar. I den frågan har det kommit ett antal väsentliga domar från Europadomstolen som har förtydligat ansvaret hos olika aktörer. Övergripande kan sägas att Europadomstolens resonemang rör vad som är önskvärt utifrån att skydda enskilda som utsätts genom hat i kommentarsfält och att samtidigt värna yttrandefriheten hos såväl enskilda som uttrycker sig i kommentarer som nyhetssidors yttrandefrihet. Det domstolen tagit hänsyn till som ett led i detta är att allt eventuellt tredjepartsansvar som läggs på exempelvis nyhetsportaler, kan leda till ett starkare skydd för enskilda men samtidigt kan det riskera att leda till att nyhetssidor helt enkelt stänger sina kommentarsfält. Det skulle då, enligt domstolen, kunna ha en negativ inverkan på yttrandefriheten. [33] Det är också ett faktum att alltfler nyhetssidor väljer att stänga ner sina kommentarsfält just för att de inte anser att de har kontroll över innehållet och kan säkerställa ett acceptabelt samtalsklimat.[34]

För att överskådligt sammanfatta de huvudsakliga resonemangen från Europadomstolen avseende hur konventionsstater ska hantera nyhetsportalers tredjepartsansvar kan framhävas betydelsen av kommentarens natur. Om det är så att kommentarerna är tydligt hotfulla och riktar sig mot individer kan det vara rimligt, enligt domstolen, att konventionsstaterna har lagstiftning som ålägger *större* nyhetsportaler ansvar att avlägsna dem och sanktioner om så inte sker. Om

[32] Avlägsnande av material i olika kontexter utreds och analyseras i Enarsson, Therese, *Avlägsnande av näthat – möjligheter, ansvar och motstående intressen*, 2017 (kommande publikation).

[33] Magyar Tartalomszolgáltatók Egyesülete och Index.hu Zrt mot Ungern (MTE och index.hu) (ansökan nr 22947/13) § 86.

[34] Se exempelvis Haidl, Kajsa, ”Fler tidningar stänger sina kommentarsfält”, *Dagens Nyheter*, publicerad på *dn.se*, 2016-04-11, Hamilton, Mary, ”The Guardian wants to engage with readers, but how we do it needs to evolve”, *The Guardian*, publicerad på *theguardian.com*, 2016-04-08, Gillinger, Christian, ”Nu dör kommentarsfälten. Igen. Men näthatet lever och frodas”, *Sveriges radio*, publicerad på *sverigesradio.se*, 2016-04-29.

det är så att kommentarerna till exempel kan anses utgöra ett hot mot samhällsordningen är det till och med aktuellt med en skyldighet att skyndsamt avlägsna materialet. Det skulle i sådana fall kunna medföra att nyhetssidor som har kommentarsfält där det finns en anledning att tro att kommentarerna kan bli hotfulla eller särskilt kränkande mot individer måste ha uppsikt över dessa för att kunna avlägsna sådant materialet.[35]

Om det istället rör sig om en mindre sida, som en mindre blogg där mängden kommentarer inte kan anses bli särskilt stor, eller där det i andra fall rör sig om exempelvis nyhetsartiklar som inte kan anses utgöra en risk för större mängder kränkande kommentarer, ska det däremot räcka att sidorna har funktioner som gör att användare kan anmäla olämpliga kommentarer. Om sådana funktioner finns kan då de som ansvarar för sidan ta ner kommentarer, i det fall det är befogat, först efter tillsägelse.[36]

I svensk lagstiftning finns ansvaret för den som tillhandahåller utrymmen på internet för att kommentera artiklar eller kommentera blogginlägg och liknande reglerat i den så kallade BBS-lagen.[37] Det innebär alltså att ansvar föreligger inte endast för den person som skrivit en olaglig kommentar, utan också för det som ansvarar för själva sidan. Ansvaret innebär att hålla uppsikt och avlägsna vissa typer av meddelanden, men endast sådana som *uppenbarligen* kan utgöra uppvigling, hets mot folkgrupp, olaga våldsskildring, barnpornografibrott och även vissa upphovsrättsbrott. Anledningen till att just dessa brottsrubriceringar ingår, och inte andra som exempelvis förtal eller ofredande, är att lagstiftaren velat inkludera sådana brott som även en lekman, utifrån objektiva kriterier i lagstiftningen, kan identifiera.[38]

Det ovanstående kan komma och ändras genom förslag som presenterades under 2016, då en statlig utredning om integritet och straffskydd initierades just på grund av de problem som uppstått i och med den explosionsartade ökningen av användandet av ny teknik. I den föreslås det bland annat att en ny brottsrubricering – olaga integritetsintrång – införs i brottsbalkens 4 kap. Förslaget syftar till att skydda individer mot särskilt svåra intrång i den personliga integriteten, som exempelvis hämndporr, det vill säga ett olovligt spridande av bild eller film av sexuell karaktär ofta på en tidigare partner. Det är sådana

[35] MTE och index.hu § 91, Delfi AS mot Estland, ansökan nr 64569/09 § 159.

[36] Se bland annat Phil mot Sverige, ansökan nr 74742/14. Resonemanget kring detta utvecklas utförligt i Enarsson, 2017.

[37] Lag (1998:112) om ansvar för elektroniska anslagstavlor. BBS står för engelskans *Bulletin Board System*.

[38] Proposition 1997/98:15 Ansvar för elektroniska anslagstavlor s. 16–17.

situationer som inte anses skyddas på ett tillfredsställande sätt genom lagstiftning.[39] Förslagen föreslås träda i kraft under år 2018.[40]

Syftet med de lämnade förslagen är dels att kriminalisera eller öka möjligheterna att rättsligt beivra vissa beteenden som tidigare varit svåra att lagföra, dels om att skärpa kraven i vissa fall för just personer som tillhandahåller exempelvis olika chattforum att hålla uppsikt och sålla bland vissa yttranden som skrivs där. Förslaget innebär att denna nya brottsrubricering, olaga integritetsintrång, och även olaga hot, ska inkluderas i det ansvar att avlägsna som numera ställs upp genom BBS-lagen.[41] Det går att ifrågasätta möjligheterna för en vanlig lekman att identifiera och bedöma om det *uppenbarligen* rör sig om ett olaga hot och olaga integritetsintrång, ett brott som, om förslaget leder till lagstiftning, är helt nytt inom svensk lagstiftning. Om det råder osäkerhet kring vad som måste avlägsnas och inte finns en risk att mer än vad som avsetts med lagstiftningen plockas bort, vilket då kan riskera att ha en kylande effekt på samtal och kommentarer på internet. Samtidigt kan förslaget som sådant, både införandet av en ny straffbestämmelse och införande av ytterligare ansvar att avlägsna kränkande uppgifter enligt BBS-lagen, innebära en stor fördel för de som utsätts för kränkningar på internet.

## 3 Framtida utveckling på näthatsområdet?

Det ovan nämnda sammanfattar några av de mest framträdande frågorna som har behandlats under projektet. Under projektets gång har det tydligt framträtt en bild av ett område som förvisso har utvecklats i en negativ riktning, där fler och fler människor uppger att de blivit utsatta, men där det samtidigt finns rättsliga möjligheter till upprättelse. Många av de kränkningar som begås på internet faller inom befintliga straffbestämmelser, och det har skett förändringar såväl avseende kriminalisering och utredning av näthat som föreslagits ytterligare sådana. Det finns också, i vissa fall, möjligheter att kräva av de som ansvarar för nyhetssidor, bloggar eller hemsidor att de ska avlägsna material. Detta innebär dock inte att brottsoffers möjligheter till upprättelse på internet i realiteten är oproblematiska. Som nämnts finns det stora skillnader i utredningsmöjligheter, och beroende av brottets natur kan ett brottsoffers enda möjlighet vara att driva ett enskilt åtal, vilket i praktiken kan vara mycket svårt eller omöjligt om

[39] SOU 2016:7 Integritet och straffskydd.

[40] Se Svt Nyheter, ”Fängelse för spridning av sexfilmer på gång”, tillgänglig på *http://www.svt.se/nyheter/lokalt/uppsala/fangelse-for-spridning-av-sexfilmer-pa-gang*.

[41] Dessa förändringar föreslås genom utredningen SOU 2016:7.

utredningen kräver teknisk bevisning som endast brottsbekämpande myndigheter kan få tillgång till. Även när utredningen drivs av polis och åklagare måste utredningsmöjligheterna användas och utredningarna prioriteras av rättsväsendet.

Det är dock tydligt att den rättsliga utvecklingen, inte bara i Sverige utan även i övriga Europa, står inför kommande utmaningar och förändringar. En av dessa är den nämnda frågan om datalagring Redan nu har den generella lagring av kommunikationsmetadata som vi haft i Sverige underkänts av EU-domstolen.[42] Det återstår att se vilka förslag på anpassning av den svenska lagstiftningen som läggs fram under år 2017 och 2018, men den typen av generell lagring som vi tidigare sett kommer med all sannolikhet inte att kunna accepteras framöver. Frågan om datalagring i förhållande till just näthat är dock även starkt kopplad till de brottsbekämpande myndigheternas möjlighet att sedan få tillgång till lagrat material. Dagens svenska ordning, där direktkontakter sker från polis eller åklagare till aktuell internet- eller mobiloperatör, har också kritiserats av EU-domstolen. Även här torde vi därför komma att se en förändring där det kommer krävas beslut från domstol eller annan oberoende myndighet för att få begära ut information från operatörer.[43]

Ytterligare en aspekt av näthat är själva ansvarsfrågan. Var ska det övergripande ansvaret ligga? Ska det uteslutande fokuseras på gärningspersonen, eller ska det ansvar som kan läggas även på andra aktörer utvidgas? Diskussionen kring ansvaret för större sociala mediaföretag har pågått under flera år, och trycket på att de ska ta ett större ansvar ökar. Så sent som i april år 2017 lades ett tyskt lagförslag fram som syftar till att ålägga sociala medieföretag mycket stora bötesbelopp om de inte avlägsnar material som utgör exempelvis *hate speech*. Ministerrådet har också under våren presenterat ett förslag som skulle medföra ansvar för stora sociala mediaföretag att avlägsna videos som innehåller *hate speech*.[44] Det skulle då vara den första lagstiftningen på EU-nivå att ålägga sådana företag ansvar för vad som publiceras på deras sidor.

Innebär det att vi framöver kommer att få se tydligare lagstiftning mot tillhandahållare? Utvecklingen nationellt och inom EU tycks gå mot att även de som tillhandahåller utrymmet för samtal, som sociala medieplattformar, måste ta

[42] Se fotnot 30.

[43] Detta har också uttalats av Sigurd Heuman, som är särskild utredare i utredningen Datalagring och EU-rätten, inför de förslag som kommer att lämnas inom ramen för uppdraget. Se ”Stopp för polisens rätt att besluta om inhämtning av teleuppgifter - ny lag om datalagring på gång”, på *Veckans juridik,* tillgängligt på *https://www.bgplay.se/video/stopp-for-polisens-ratt-att-besluta-om-inhamtning-av-teleuppgifter-ny-lag-om-datalagring-pa-gang*, publicerad 2017-04-11.

[44] Förslaget har ännu inte i skrivande stund behandlats av Europaparlamentet.

ett ansvar för det som publiceras där. Detta kan ge god effekt då, i vart fall de största, sociala medieplattformarna är vinstdrivande och har stora resurser, och därmed också möjlighet att bevaka innehållet. Även om företagen inte blir straffrättsligt är ansvariga, så kan det vara ett effektivt sätt att hantera frågan och det belastar dessutom den privata utövare som möjliggjort att problemet uppstått. Samtidigt kan det, som nämnts ovan, vara viktigt för brottsoffret att frågorna hanteras genom en straffrättslig process gentemot gärningspersonen. Dessa olika sätt att hantera näthat torde dock inte stå i konflikt med varandra.

Det går också redan nu att utläsa ett skifte mot ett tydligare ansvar på aktörer genom EU-domstolens dom i Google Spain mot AEPD och Mario Costeja González (Google Spain).[45] Kortfattat slog där domstolen fast att Google, och rimligen andra större sökmotorer, var skyldiga att beakta önskemål från enskilda som ville att sökresultat om dem inte längre skulle visas. I och med detta kan enskilda få större inflytande över informationen om den egna personen och sökmotorer kan vara tvungna att avlägsna material så att det inte längre är sökbart. Materialet som sådant avlägsnas dock inte. I fråga om näthat kan det ha betydelse för den enskilda att kränkande uppgifter som är svåra för den enskilda att få avlägsnat i vart fall är svårare att hitta på internet. Genom EU:s dataskyddsförordning som i maj år 2018 ersätter den svenska personuppgiftslagen (PUL), finns också, under vissa förutsättningar, ett uttryckligt skydd för vad som där benämns ”rätten att raderas” vilket kan omfatta liknande rättigheter för den enskilda.[46] Hur förordningen kommer tolkas och implementeras på nationell nivå återstår dock att se. I nuläget och fram till att den nya förordningen träder i kraft skyddas dock redan information om den enskilda – utifrån svensk rätt – genom bestämmelser i just PUL som implementerade dataskyddsdirektivet i svensk rätt.

Avslutningsvis är det viktigt att poängtera att det i nuläget på såväl nationell och europeisk nivå sker förändringar gällande synen på näthat och hur det ska hanteras rättsligt. Utvecklingen på internet har i praktiken tvingat fram lagstiftningsåtgärder, då fenomenet har blivit ett samhällsproblem. Det är dock av stor vikt att inte endast behandla frågan på lagstiftnings- och samhällsnivå utan också på individnivå. Att området präglas av kontextuella faktorer, och att en

[45] Mål C-131/12, Google Spain SL och Google Inc. mot Agencia Española de Protección de Datos (AEPD) och Mario Costeja González, EU:C:2014:317.

[46] Se Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning). Detta utvecklas också i Enarsson, 2017.

enskild händelse kan präglas av det i samtliga led, från sammanhanget kring själva händelsen som sådan, genom utredning och till bedömning i domstol, gör att den rättsliga hanteringen av brottet kan vara svår att förstå för någon som kränks på internet. Det kan vara mycket svårt för en enskild person att förstå varför vissa uttalanden ibland tycks vara tillåtna och ibland inte alls, eller varför spridande av information om andra människor kan vara tillåtet, till och med påbjudet, i vissa sammanhang men olagligt i andra. Avslutningsvis är det därför viktigt att poängtera vikten av att polis och åklagare, som främst har kontakt med ett brottsoffer under utredningen, är tydliga med varför beslut fattas. För att kunna åstadkomma detta krävs också ökad kunskap och resurser för att kunna utreda och lagföra brotten. På individnivå i detta av stor vikt för att i största mån hjälpa de som utsätts för näthat.