Juridisk Publikation
STOCKHOLM - UPPSALA - LUND - GÖTEBORG - UMEÅ

Paulina Rehbinder

Att väva det mörka nätet
– straffrättsliga aspekter av att tillhandahålla tor-noder

Särtryck ur häfte 1/2017

Nummer 1/2017

ATT VÄVA DET MÖRKA NÄTET

– STRAFFRÄTTSLIGA ASPEKTER AV ATT TILLHANDAHÅLLA TOR-NODER

Av Paulina Rehbinder[1]

Anonymitet och övervakning har under internets utveckling varit en ständigt brännande fråga där yttrandefrihet och brottsbekämpande ofta ställts mot varandra. Samtidigt har medvetenheten om övervakning och den personliga integriteten ökat i samhället, men också lagstiftarens intresse för brotts- och terrorbekämpning. Möjligheterna att gömma sig själv och information via Darknet och på Deep web ställer inte bara större krav på rättsvårdande myndigheter. Risken att bli utsatt för angrepp via internet ökar, utan att någon därefter kan ställas till svars. Tor-nätverket, som används både för skydd mot staters övergrepp på individer och av kriminella för att gömma sig från rättsvårdande myndigheter, ställer dessa frågor på sin spets där grundläggande rättigheter som yttrandefrihet och integritet vägs mot samhällsintressen som säkerhet och trygghet. Denna betraktelse syftar till att ge en överblick av det straffrättsliga ansvar tillhandahållare av Tor-noder kan åläggas oaktat vilka intentioner som ligger bakom tillhandahållandet.

1. INLEDNING

Tor[2] är en anonymiseringstjänst som möjliggör för användare att surfa på internet utan att trafiken till och från användares datorer kan spåras direkt till dennes IP-adress. Anonymiteten uppnås genom att trafiken krypteras i och överförs via så kallade Tor-noder vars IP-adresser nyttjas och anonymitet möjliggörs. Tor-noderna fungerar som knutpunkter för trafiken i Tor-nätverket där trafiken dirigeras, på samma sätt som noderna i bredbandsnätet.

För att nätverket ska kunna fungera krävs att det tillhandahålls så kallade Tor-noder som bildar nätverket. Ju fler Tor-noder det finns desto snabbare kan trafiken gå i nätverket. Vem som helst som har tillgång till bredband och en lagringsenhet (exempelvis en dator eller server) har möjlighet att skapa en

1 Jurist och grundare av juristbyrån it girl law inom vilken rapporten ”Tillhandahållande av Tor-noder – rättsliga aspekter” skrevs på uppdrag av Journalistförbundet med finansiering av Internetfonden. Denna betraktelse är en omarbetning av rapporten. Jag vill rikta ett särskilt tack till advokat Fredrik Engström som har bidragit med goda synpunkter på innehållet i både rapporten och i betraktelsen.

2 Se officiell hemsida för Tor, https://www.torproject.org/, senast hämtad 2017-04-02.

Tor-nod och i dag är det både privatpersoner och juridiska personer som tillhandahåller Tor-noder.

Anonymitet är inte alla gånger självvald: journalister har exempelvis en grundlagsfäst plikt att skydda sina källor, något som framgår av tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Vikten av att upprätthålla anonymitet är särskilt viktig i de länder där internet är hårt övervakat av staten.[3] I dessa länder kan anonymiteten vara en fråga om liv eller död.[4] Frågan om just staters övervakning av internet blev högst aktuellt då Edward Snowden den 5 juni 2013 avslöjade att den amerikanska staten bedrev massövervakning av allt ifrån sina medborgare, till politiska ledare runt om i världen.[5] Exempel på användare av Tor är: privatpersoner som vill skydda sig från övervakning på internet, företag som vill skydda sin verksamhet från insyn från konkurrenter, aktivister som vill kunna skydda sig från strängt övervakande stater, journalister som har en skyldighet att skydda sina källor, och militären samt rättsvårdande myndigheter som behöver skydda sin kommunikation och i vissa fall informationsinhämtande på internet.[6] Det gemensamma intresset för samtliga användare kan sägas vara att skydda sina aktiviteter på internet från insyn.

Möjligheten till anonymitet har dock kommit att skapa bekymmer hos främst rättsvårdande myndigheter eftersom anonymiteten försvårar utredning och beivrande av brott. I dag sker exempelvis nästintill alla barnpornografibrott på internet varför det är avgörande för de rättsvårdande myndigheterna att kunna spåra, säkra bevis och identifiera användarna som besökt hemsidor med sådant material.[7]

I det fall att någon användare utnyttjar Tor när de begår brott på internet, är det den IP-adress som tillhandahållaren av utgångsnoden i Tor-nätverket har som rättsvårdande myndigheter kan se. Detta innebär att rättsvårdande myndigheter kan komma att kontakta tillhandahållaren av utgångsnoden eftersom det ser ut som att det är tillhandahållaren som exempelvis har besökt en hemsida med barnpornografi. Det är därför av intresse att utröna om, och

3 Andersson, Sus, Laurin, Fredrik och Jankov, Petra, Digitalt källskydd – en introduktion, s. 53, https://www.iis.se/docs/digitalt-kallskydd-2.pdf, senast hämtad 2017-04-22.
4 Andersson m.fl., s. 21.
5 MacAskill, Ewen och Ackerman, Spencer, NSA collecting phone records of millions of Verizon customers daily, The Guardian, den 6 juni 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order, senast hämtad 2017-04-22.
6 Se officiell hemsida för Tor, https://www.torproject.org/, senast hämtad 2017-04-22.
7 It-relaterade brott - polisens arbete, senast uppdaterad den 8 december 2014 kl. 15:54, https://polisen.se/Om-polisen/Olika-typer-av-brott/IT-brott/, senast hämtad 2017-04-22.

i så fall när, en tillhandahållare av Tor-noder kan komma att hållas straffrättsligt ansvarig för tillhandahållandet av Tor-noder även om det är användaren som har utfört själva gärningen.

Betraktelsen inleds med en teknisk beskrivning av Tor-nätverket i syfte att ge läsaren en förståelse för tekniken eftersom den spelar en avgörande roll för den juridiska analysen. Därefter presenteras den juridiska analysen av straffrättsligt ansvar för tillhandahållande av Tor-noder både som huvudgärning och för medverkan, varpå en redogörelse för tillämpligheten av social adekvans följer. Betraktelsen avslutas med en kortare summering av slutsatserna samt en reflektion.

2. ÄR TOR EN FRISTAD FÖR KRIMINELLA?

Tor förknippas av allmänheten många gånger med brottslig verksamhet på internet och begrepp som *Deep web* och *Darknet* dyker ibland upp i diskussioner om Tor. Dessa begrepp behöver därför kort förklaras.

Deep web utgör den del av internet som inte är indexerat, vilket enkelt uttryckt betyder att det genom en vanlig sökmotor inte går att hitta resultaten från *Deep web*; innehållet blir då endast tillgängligt om hela adressen skrivs in i adressfältet i webbläsaren. Det saknas i dag entydiga uppgifter om hur stor del av innehållet på hela internet som utgör olagligt material eller hur stor del av all trafik på internet som är kopplad till brott, precis på samma sätt som den informationen saknas för *Deep web*.

Termen *Darknet* används ibland för Tor eftersom Tor-nätverket anses utgöra ett *Darknet*. Namnet till trots innebär nämligen *Darknet* egentligen bara att användare behöver en viss typ av mjukvara för att få tillgång till nätverket, varför det i fallet med Tor innebär att användaren behöver konfigurera sin enhet med Tor-mjukvaran för att få tillgång till Tor. Det finns även andra *Darknet* som satts upp i syfte att exempelvis dela filer inom nätverket, vilket eventuellt leder tankarna till nätverk som delar olagligt material. Även om så skulle vara fallet innebär det inte att alla *Darknets* utnyttjas för sådana syften.

Att Tor-nätverket har figurerat i media – t.ex. i samband med tillslaget mot hemsidan Silk Road[8] (en marknadsplats för allt från droger till lönnmördare) – har troligtvis påverkat allmänhetens uppfattning. Men det finns i dag inga erkända uppgifter eller bevis för att en större del

8 Bie, Nanok, FBI stängde ökänd drog- och vapenhandelssajt, SVT Nyheter, den 2 oktober 2013, uppdaterad den 9 oktober 2013, http://www.svt.se/nyheter/utrikes/okanda-drog-och-vapenhandelssajten-silk-road-nedstangd, senast hämtad 2017-04-22.

av trafiken i Tor är kopplad till brottslig verksamhet än trafiken på internet generellt.

3. TEKNIKEN

3.1 TOR – BAKGRUND OCH UPPKOMST

Tor är en anonymiseringstjänst där användaren genom tre lager av krypteringstunnlar kan surfa på internet utan att trafiken kan spåras direkt till användaren. Nätverket bygger på noder där användare kan utnyttja bandbredd och IP-adresser från de som tillhandahåller Tor-noder.

För att kunna få tillgång till Tor-nätverket behöver användaren ladda ner en mjukvara som tillhandahålls gratis på hemsidan till Tor-project. År 2006 startades den ideella organisationen Tor-project som i dagsläget driver utvecklingen av mjukvaran och även sköter marknadsföring och opinionsbildning kring Tor. Mjukvaran skapades och utvecklades från början av U.S. Naval Research Laboratory (”NRL”) i mitten av 1990-talet, i syfte att säkra skyddet för den amerikanska flottans kommunikation.[9]

I början av 2000-talet gav NRL ut koden gratis som en öppen programvara.[10] Från att tidigare helt finansierats och utvecklats av den amerikanska staten tog nu Electronic Frontier Foundation över organiseringen av utvecklingen av Tor. Tor finansieras dock fortfarande av diverse stater, organisationer och privatpersoner även om det nu är Tor-project som står för utvecklingen av Tor. Den svenska biståndsmyndigheten Sida var en av finansiärerna av Tor mellan åren 2010–2013.[11]

I dag finns det dagligen strax över två miljoner användare av Tor, men denna siffra förändras kontinuerligt.[12]

9 Översikt av Tor, https://www.torproject.org/about/overview, senast hämtad 2017-04-22.

10 Meddelande om lansering av ”onion router”, publicerat den 20 september 2002, http://archives.seul.org/or/dev/Sep-2002/msg00019.html, senast hämtad 2017-04-22, Meddelande om lansering av Tor, publicerat den 8 oktober 2003, https://lists.torproject.org/pipermail/tor-dev/2003-October/002185.html, senast hämtad 2017-04-22, Levine, Yasha, Almost everyone involved in developing Tor was (or is) funded by the US government, Panodaily, publicerat den 16 juli 2014, http://pando.com/2014/07/16/tor-spooks/, senast hämtad 2017-04-22, Skärmutklipp från den officiella hemsidan för Tor, https://www.evernote.com/shard/s1/sh/23cf697d-2353-4247-815c-b4efa35d8639/3ade44b5db780f279f550f9e6ecbb2ac, senast hämtad 2017-04-22.

11 Officiell lista över finansiärer av Tor, https://www.torproject.org/about/sponsors.html.en, senast hämtad 2017-04-22.

12 Statistik över användare av Tor, https://metrics.torproject.org/userstats-relay-country.html?graph=userstats-relay-country&start=2012-01-01&end=2015-02-16&country=all&events=off,

3.1.1 NÄTVERKET

De som vill använda Tor kan välja att antingen bara utnyttja nätverket och då vara en *klient*[13] eller tillhandahålla Tor-noder och då vara *tillhandahållare*.[14] För att bli klient i Tor behöver användaren ladda ner Tor-mjukvaran till sin enhet[15] och konfigurera den i enlighet med mjukvaran. På så sätt kan användaren använda sig av Tor på internet utan att användarens egen IP-adress syns. Som klient går det även att tillhandahålla hemsidor utan att det går att spåra varifrån hemsidan drivs (så kallade *hidden services*[16]).

Den andra rollen är tillhandahållare av Tor-noder och uppnås genom att likt ovan beskrivits konfigurera en enhet men nu istället till en Tor-nod. Genom denna konfiguration kan enheten dela med sig av bandbredd och sin IP-adress till andra Tor-klienter.

Tillhandahållare av Tor-noder avgör själv hur mycket bandbredd noden ska dela med sig av till klienterna i Tor. Den bandbredd som tillhandahålls genom driften av Tor-noder betalar tillhandahållarna för hos sin internetleverantör (”ISP”). Genom att låta klienter utnyttja den bandbredd som tillhandahållare betalar för, tillåts de också utnyttja den IP-adress som tillhandahållaren har på sin enhet. Frågan om tillhandahållande av IP-adress till klienter blir mest relevant för dem som driver utgångsnoder eftersom det är trafiken från dessa noder som ser ut att vara avsändare av trafik som lämnar Tor-nätverket.

Tor-nätverket bygger på tre typer av noder: ingångsnod, mellannod och utgångsnod.

3.1.2 CONSENSUS

Trots att en enhet är konfigurerad innebär det inte att noden används kontinuerligt i Tor-nätverket. När tillhandahållaren konfigurerat sin enhet skickas information om att noden är tillgänglig till ”directory authorities” (”DA”).[17] DA är noder konfigurerade att samla upp information om samtliga

---

senast hämtad 2017-04-22.

13 Benämningen ”klient” syftar på den enhet som användaren konfigurerat för att kunna utnyttja Tor och benämningen ”användare” syftar på de fysiska personer som står bakom ”klienterna” i Tor.

14 Även om tillhandahållare själva kan använda Tor, kommer definitionen ”tillhandahållare” i denna betraktelse att användas för de som tillhandahåller Tor-noder i nätverket.

15 Någon form av lagringsmedia, exempelvis en vanlig hemmadator eller en hyrd server i en serverhall.

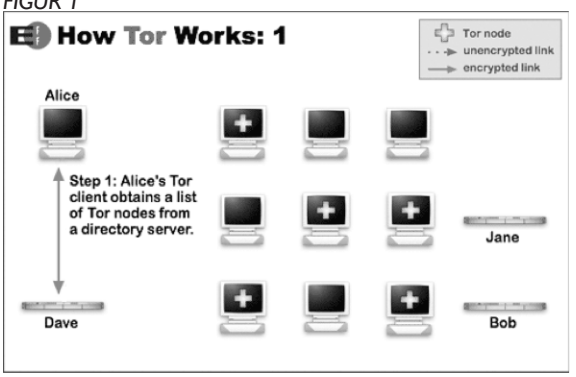
16 Officiell hemsida för Tor, ”hidden services”, https://www.torproject.org/about/overview.html.en#hiddenservices, senast hämtad 2017-04-22.

17 Det kan nämnas att det finns nio stycken DA, se https://metrics.torproject.org/about.html,

Tor-noder som är tillgängliga samt nodernas egenskaper[18]. DA skapar och publicerar sedan *consensus* en gång i timmen genom en automatiskt förprogrammerad procedur[19]. *Consensus* är en offentlig lista över alla Tor-noder och visar även vilken typ noderna är.[20] Samtliga Tor-noder går alltså att se i *consensus*.[21] *Consensus* hämtas av samtliga klienter så att klienternas enheter vet till vilka noder trafik kan skickas. Genom att DA tilldelar noderna sina roller kan den som driver noder inte på egen hand avgöra vilken typ av nod de för tillfället ska tillhandahålla. Samtliga klienter i Tor hämtar automatiskt *consensus* så snart den skapas. Klientens enhet får då information om vilka noder som är aktiva i nätverket och var trafiken från enheten kan skickas.

3.1.3 HUR FUNGERAR TOR?

FIGUR 1[22]



Ponera att användaren vill besöka hemsidan www.sverigesradio.se. När användaren skriver in adressen i webbläsaren skickas informationen till en ingångsnod

senast hämtad 2017-04-22.

18 En egenskap kan exempelvis vara hur mycket bandbredd noden tillhandahåller och vilken typ av funktion enheten är konfigurerad för.

19 Proceduren innebär att samtliga DA röstar fram *consensus* genom en programmerad algoritm. Det saknas behov av fördjupning i algoritmerna och programmeringen av dessa för den fortsatta framställningen i denna betraktelse, varför detta kommer att utelämnas.

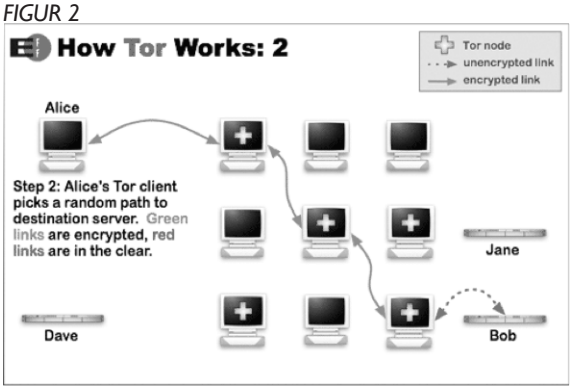
20 Se *consensus* och dess statistik, https://consensus-health.torproject.org/, senast hämtad 2017-04-22.

21 Det finns dock så kallade *bryggnoder* som inte publiceras i *consensus*, men dessa kommer inte att beröras i denna betraktelse.

22 Översikt av Tor, https://www.torproject.org/about/overview. Figur 1,2 och 4 får publiceras i enlighet med Creative Commons Attribution 3.0, https://creativecommons.org/licenses/by/3.0/us/, senast hämtad 2017-04-22.

genom en krypterad tunnel som skapas mellan klienten och ingångsnoden. Det utfärdas en uppsättning krypteringsnycklar för denna tunnel. Den enda information ingångsnoden får är varifrån trafiken kom och vilken mellannod trafiken ska skickas till. Därefter skapas det ytterligare en krypteringstunnel mellan klienten och mellannoden och en ny uppsättning krypteringsnycklar för just den tunneln skapas. Den enda information mellannoden får är att trafiken kom från ingångsnoden och att den ska till en viss utgångsnod. Därefter skapas ytterligare en krypteringstunnel mellan klienten och utgångsnoden. Även för denna tunnel skapas en ny uppsättning krypteringsnycklar. Samtliga krypteringsnycklar förhandlas alltså fram mellan klienten och respektive Tor-nod enskilt genom en avancerad krypteringsteknik[23] utan att klientens identitet framgår.

FIGUR 2

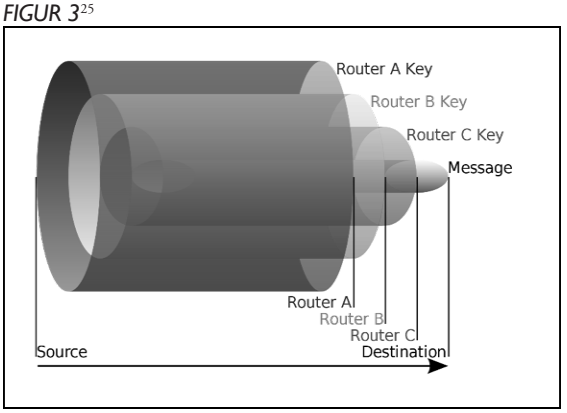


Som beskrivits har ingen nod den fullständiga informationen om varifrån trafiken ursprungligen kom eller vad som är trafikens slutdestination. Detta innebär att ingen kan spåra klientens trafik genom att hacka sig in och övervaka någon av noderna enskilt. Krypteringen i Tor fungerar som beskrivits ovan som skalen på en lök och Tor utgör därför ett ”onion router”[24]-nätverk.

23 Krypteringssystemet kallas Diffie–Hellman, senast uppdaterad den 22 mars 2017, https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange#Description, senast hämtad 2017-04-22.

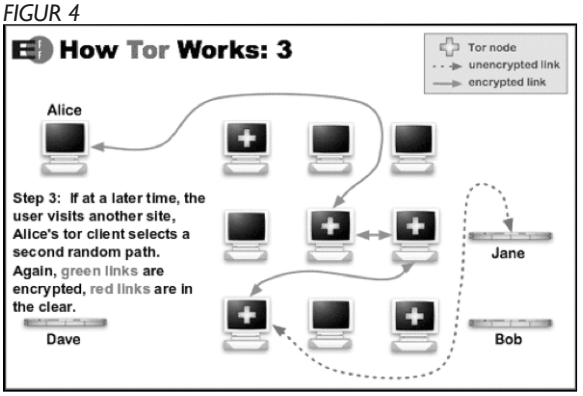
24 Hemsida om ”onion routing”, historisk exposé, http://www.onion-router.net/History.html, senast hämtad 2017-04-22.

FIGUR 3[25]



När trafiken slutligen når utgångsnoden och lämnar Tor-nätverket upphör krypteringen som Tor tillför. Den som bevakar slutmålet för trafiken eller utgångsnoden kan då se trafiken från utgångsnoden och var trafiken går. Det innebär att meddelanden som skickas och tas emot, måste krypteras i sig för att de ska vara skyddade från insyn när meddelandena lämnar Tor.

FIGUR 4



Vägvalet för trafiken är som ovan beskrivits inget klienten ser eller märker av, utan enheterna kommunicerar och överför trafik till varandra och utan

25 Bilden är hämtad från English Wikipedia-användaren HANtwister och får publiceras i enlighet med Creative Commons Attribution-Share Alike 3.0 Unported license, https://creativecommons.org/licenses/by-sa/3.0/, https://upload.wikimedia.org/wikipedia/commons/thumb/e/e1/Onion_diagram.svg/2000px-Onion_diagram.svg.png, senast hämtad 2017-04-22.

inblandning av användaren eller tillhandahållaren. Klienten kan dock i viss mån påverka vilka Tor-noder som ska användas eller inte användas.

Det är utgångsnodens IP-adress som kommer att framstå som besökare av en viss hemsida eller sändare av ett visst meddelande trots att det är en Tor-klient med en annan IP-adress vars trafik går till hemsidan eller skickar meddelandet. Rättsvårdande myndigheter kan därför komma att misstänka tillhandahållaren av utgångsnoden för att besöka sidor med olagligt innehåll och dylikt.

Den som tillhandahåller utgångsnoder kan använda en så kallad "exit policy" där vissa tjänster, nätverk eller tillhandahållare av slutdestinationer kan blockeras.[26] Det kan dock påpekas att de flesta som använder Tor och framförallt de som utför brott via internet troligtvis använder sig av ytterligare kryptering utöver Tor, varför exit policyn sällan kan stoppa överföring av trafik till exempelvis hemsidor med olagligt material.

4. STRAFFRÄTTSLIGA ASPEKTER

4.1 INLEDNING

När nya fenomen uppkommer i samhället ställs jurister alltid inför frågan, hur nuvarande lagstiftning ska appliceras på fenomenet. Digitaliseringen gjorde intåg för flera decennier sedan men fortfarande kämpar jurister med att inordna digitala lösningar i en analog lagstiftning. Oavsett fenomen ska dock *legalitetsprincipen* alltid iakttas vid straffrättsliga bedömningar.[27]

Legalitetsprincipen ställer upp fyra krav, eller begränsningar, för att straffbarhet ska uppkomma: 1) krav på att *vad som utgör brott ska vara föreskrivet* och att det ska finnas ett föreskrivet straff för detta, 2) *retroaktivitetsförbud*, att nya bestämmelser inte får användas för att straffa någon för en gärning som när den utfördes inte var straffbar, 3) *analogiförbud*, att en straffrättslig bestämmelse inte får utvidgas utöver ordalydelsen i bestämmelsen, och 4) *obestämdhetsförbud*, att en bestämmelse måste gå att förstå och vara tillräckligt precis.[28]

Frågor om brottsbekämpande väcker ofta starka känslor och legalitetsprincipen riskerar i diskussioner om detta att glömmas bort. Jag vill därför understryka att oavsett åsikt om Tor eller brottsbekämpning ska de gränser

26 Tor FAQ, https://www.torproject.org/docs/faq.html.en#ExitPolicies, senast hämtad 2017-04-22.

27 SOU 1988:7, *Frihet från ansvar – Om legalitetsprincipen och om allmänna grunder för ansvarsfrihet*, s. 43.

28 Asp, Petter, Ulväng, Magnus och Jareborg, Nils, *Kriminalrättens grunder*, 2., omarb. uppl., Iustus, Uppsala, 2013, s. 46.

som legalitetsprincipen ställer upp, enligt min uppfattning, aldrig överträdas i ett demokratiskt samhälle.

Eftersom internet möjliggör att brott kan begås på flera platser i världen samtidigt utan att gärningspersonen behöver närvara fysiskt på dessa platser, uppstår jurisdiktionsfrågor. Den fortsatta redogörelsen i denna betraktelse kommer därför att göras ur ett nationellt perspektiv där det förutsätts att Tor-noderna är placerade i Sverige, att gärningspersonen befinner sig i Sverige samt att platsen för brottets fullbordan är Sverige, för att löpande i redogörelsen undvika frågor om jurisdiktion.

4.2 INTERNET SOM BROTTSPLATS

Flertalet brott kan i dag begås via internet, bland annat barnpornografibrott, olaga hot och bedrägeri.[29] Svea hovrätt har tidigare uttalat att våldtäkt skulle kunna begås via internet när en person uppmanar någon annan att utföra sexuella handlingar på sig själv även om någon ännu inte blivit dömd för detta.[30] Slutsatsen drog Svea hovrätt baserat på en tidigare dom[31] från Högsta domstolen (”HD”) där det fastställdes att det inte krävs fysisk närvaro för att kunna bli dömd för sexuellt övergrepp mot barn[32]. Frågan om bland annat sexuellt övergrepp mot barn via internet avgjordes återigen av Svea hovrätt i mars 2016.[33] Frågan om brotten kunde utföras över internet var i detta avgörande inte någon reell fråga för rätten utan bedömdes vara en vedertagen möjlighet och den åtalade personen dömdes av Svea hovrätt för de inträffade händelserna. I ett mål från Attunda tingsrätt friades en person för våldtäkt mot barn över internet eftersom den åtalade personen inte varit närvarande via internet när de sexuella handlingarna utfördes.[34] Den åtalade personen dömdes dock för flera andra brott, bland annat sexuellt övergrepp mot barn, utnyttjande av barn för sexuell posering, sexuellt ofredande, och barnpornografibrott.[35]

29 BrB 16:10 a, BrB 4:5 och BrB 9:1. Notera även distinktionen mellan brott som begås på internet som vanligen kallas för ”IT-relaterade brott” medan begreppet ”IT-brott” normalt används för att beteckna dataintrång eller datorbedrägeri, se It-relaterade brott - polisens arbete, https://polisen.se/Om-polisen/Olika-typer-av-brott/IT-brott/, senast hämtad 2017-04-22.
30 Svea hovrätt, dom den 2015-09-09, mål nr B 6051-15, s. 8.
31 NJA 2015 s. 501, s. 5-7.
32 BrB 6:6.
33 Svea hovrätt, dom den 2016-03-01, mål nr B 5801-15.
34 Attunda tingsrätt, dom den 2016-06-23, mål nr B 1687-14, s. 52.
35 BrB 6:8, BrB 6:10 och BrB 16:10 a.

4.3 KAN TILLHANDAHÅLLANDE AV TOR-NODER INNEBÄRA ETT BROTT?

För att kunna göra en straffrättslig bedömning av tillhandahållande av Tor-noder behöver det inledningsvis fastställas vad tillhandahållandet av Tor-noder innebär juridiskt och inte bara tekniskt.

Det bör här även inflikas att IP-adresser har ansetts vara personuppgifter i de fall IP-adressen har kunnat kopplas till en fysisk person. En IP-adress kan på så sätt likställas med ett telefonnummer och därmed skulle tillhandahållandet av IP-adress genom Tor-noder kunna jämställas med att låna ut en telefon. Att låna ut sin telefon till någon som begår ett brott, exempelvis hotar någon via telefon, kan i sig inte innebära något brott. Däremot kan det i vissa fall utgöra medverkan till brott. Det bör därför inledningsvis understrykas att utlånande av IP-adress således i sig inte innebär något brott.

4.3.1 SKYDDANDE AV BROTTSLING

Då tillhandahållare av Tor-noder erbjuder ett verktyg för anonymitet kan det i de fall någon begår ett brott och vill skydda sin identitet innebära att tillhandahållaren av Tor-noder erbjuder en möjlighet att försvåra identifiering av gärningspersonen. Frågan blir således om det kan anses vara ett brott att försvåra identifiering av någon som begår brott.

Den brottsbeskrivning som ligger närmast till hands är *skyddande av brottsling* vilket framgår av BrB 17:11 st. 1:

> ”Om någon döljer den som förövat brott, hjälper honom eller henne att undkomma, undanröjer bevis om brottet eller på annat dylikt sätt motverkar att det uppdagas eller beivras, döms för skyddande av brottsling till böter eller fängelse i högst ett år.”

Brottet kan alltså begås antingen genom att dölja en gärningsperson eller genom att dölja själva brottet. Döljande av brott är exempelvis att avlägsna spår från en gärningsplats såsom finger- eller fotavtryck,[36] och döljande av gärningspersonen innebär att motverka att brott upptäcks eller att gärningspersonen upptäcks, blir föremål för utredning, lagföring, dom eller verkställighet av straff.[37]

36 Nilsson, Göran, *Brottsbalk (1962:700) 17 kap. 11 §,* Lexino 2015-08-01, 2.2.3.
37 Nilsson, *Brottsbalk (1962:700) 17 kap. 11 §,* Lexino 2015-08-01, 2.2.4.

För personligt ansvar krävs uppsåt till både att en annan person begått ett brott och att den egna handlingen som vidtagits skett i syfte att dölja brott eller försvåra utredning och lagföring.[38]

I BrB 17:11 st. 4 föreskrivs dock att det räcker med oaktsamhet (”*inte insåg men hade skälig anledning att anta*”) i förhållande till att en person begått ett brott för att bli personligt ansvarig. Detta innebär dock fortfarande att handlingen att dölja eller försvåra upptäckt, beivrande och straffande av brott måste vara täckta av uppsåt avseende de handlingar som vidtagits av den som döljer.[39]

Enligt bestämmelsen krävs det att döljandet sker efter att ett brott har begåtts, samt att den som döljer känner till eller hade skälig anledning att anta vilken gärning huvudgärningspersonen utfört för att ansvar ska kunna uppkomma. Tillhandahållande av Tor-noder möjliggör anonymitet för användare under tiden de utför brott över internet. Detta innebär att den döljande handlingen från tillhandahållare av Tor-noder upphör då användarens trafik inte längre överförs via tillhandahållarens Tor-nod, varför tillhandahållandet av Tor-noder inte utgör ett döljande i lagstiftningens mening. Tillhandahållaren känner inte heller till vilka gärningar som användaren utför genom användningen av Tor-noderna varför tillhandahållare inte kan anses ha sådan kännedom eller kunna få sådan anledning att anta som krävs för att kunna hållas ansvariga för skyddande av brottsling. Tillhandahållare av Tor-noder bör mot bakgrund av ovan därför inte kunna hållas ansvariga för skyddande av brottsling.

4.4 MEDVERKAN

Det krävs generellt inget särskilt stadgande för att medverkan till brott ska vara straffbart, inte heller krävs det att gärningspersonen har identifierats för att personligt ansvar för medverkan ska uppkomma.[40] Däremot krävs att det finns en gärningsperson och att det kan fastställas att denne har utfört en *otillåten gärning*; det krävs alltså inte att gärningspersonen har ådragit sig personligt ansvar för sitt handlande.[41] I The Pirate Bay-domen (”TPB-domen”)[42] konstaterade Svea hovrätt exempelvis att det var styrkt att det fanns gärningspersoner, men att dessa var okända.[43]

38 Nilsson, *Brottsbalk (1962:700) 17 kap. 11 §,* Lexino 2015-08-01, 2.4.1.
39 Nilsson, *Brottsbalk (1962:700) 17 kap. 11 §,* Lexino 2015-08-01, 2.2.4.
40 Asp, Ulväng och Jareborg, s. 430.
41 Asp, Ulväng och Jareborg, s. 436, det kan alltså ha förelegat en ursäktande omständighet för huvudgärningspersonen varför denne kan undgå ansvar samtidigt som en annan person kan hållas ansvarig för medverkan.
42 Svea hovrätt, dom den 2010-11-26, mål nr B 4041-09.
43 TPB-domen, s. 17.

Medgärningspersonen behöver endast ha uppsåt till den konkreta gärningen som utgör huvudbrottet, varför det inte krävs fullständig överensstämmelse mellan medgärningspersonens uppfattning och det verkliga händelseförloppet. Detta innebär att medverkanspersonen kan bli ansvarig för medverkan till ett annat brott än det som huvudgärningspersonen utfört.[44] Det krävs dock att gärningspersonen utfört en otillåten handling för att medverkanspersonen ska kunna hållas ansvarig; skulle det visa sig att gärningspersonen saknat uppsåt eller av någon annan anledning inte ska straffas för sitt agerande kan ansvar fortfarande alltså åläggas en medverkansperson.[45]

För att över huvud taget kunna bli föremål för misstanke om medverkan krävs att det föreligger ett klart samband mellan medverkanspersonens främjande och gärningen som utgör huvudbrottet.[46] Det ställs alltså krav på kausalitet mellan medverkanspersonens påverkan och gärningspersonens gärningar. Främjandet kan ske både genom att medverkanspersonen utför en handling eller genom att underlåta att göra något.[47]

Något kort ska här nämnas om medverkan genom underlåtenhet. Eftersom det inte finns någon allmän skyldighet att ingripa mot annans brott krävs för ansvar att medverkanspersonen vid fysisk medverkan har en skyldighet till det enligt lag, avtal eller genom så kallad garantställning[48].[49] Det saknas en sådan skyldighet för tillhandahållare av Tor-noder baserat på lag eller avtal, och ansvar genom garantställning blir inte aktuellt för tillhandahållare av Tor-noder.[50] Medverkansansvar genom underlåtenhet kommer därför inte att beröras närmare i denna artikel.

4.4.1 ANSTIFTAN

Anstiftan är en form av medverkan och innebär att någon genom psykisk påverkan förmår någon annan att handla på ett visst sätt. Det räcker med att ge gärningspersonen tillräckliga skäl att handla för att det ska anses vara anstiftan.[51] En straffbar anstiftan förutsätter att anstiftaren hos en annan person framkallat beslut att begå brott; det krävs alltså en form av psykiskt

44 NJA 2007 s. 929.

45 För en bättre förståelse för otillåten gärning och straffbarhet se Asp, Petter och Ulväng, Magnus, *Täckningsprincipens ABC*, Juridisk Publikation 2/2009 [265–273].

46 Nicander, Hans, *Upphovsrätten och medverkansansvaret i en digital miljö*, SvJT 2012 [258–281] s. 260.

47 Asp, Ulväng och Jareborg, s. 430.

48 Exempelvis vårdnadshavare eller badvakt, se även BrB 23:6.

49 Se även NJA 2003 s. 473 för vidare resonemang.

50 SOU 1996:185, *Straffansvarets gränser Del 1, Betänkande från Straffansvarsutredningen*, s. 311 ff.

51 Asp, Ulväng och Jareborg, s. 441.

samband mellan medverkanspersonens påverkan och gärningspersonens handlande. Saknas det psykiskt samband, exempelvis därför att gärningspersonen redan tidigare haft för avsikt att begå det anstiftade brottet, rör det sig inte om anstiftan.[52] Medverkansansvar blir alltså inte aktuellt för tillhandahållare av Tor-noder om gärningspersonen redan innan denne kände till Tor hade för avsikt att begå brottet utan möjligheten till anonymitet genom Tor.

I praxis har psykisk påverkan bland annat ansetts vara att någon pressat någon annan att ändra sitt vittnesmål[53] eller att uppdra åt någon att genomföra ett brott samt lämna nödvändig information för att brottet skulle kunna fullbordas[54]. Det som är gemensamt för målen om anstiftan är att det har skett en korrespondens mellan medverkanspersonen och gärningspersonen (eller i ett led till denne) där information om vilken handling eller vilket resultat som den otillåtna gärningen ska utgöra har lämnats. Det psykiska sambandet bör alltså anses innefatta någon form av reell uppfattning om vad som ska ske och ska förmedlas mellan personerna.

Tillhandahållare av Tor-noder står inte i någon kontakt med användarna av Tor annat än att deras enheter korresponderar. Genom bristen på innehållsmässig korrespondens[55] mellan tillhandahållarna och användarna av Tor bör det inte kunna anses som att tillhandahållare genom att tillhandahålla Tor-noder kan ha en sådan psykisk påverkan på användarna att det inryms i begreppet anstiftan.

Erbjudande om anonymitet kan säkerligen påverka en person som överväger att begå ett brott att skrida till verket i hopp om att inte bli upptäckt eller försvåra upptäckten av brott. Om så skulle vara fallet kan tillhandahållaren ändå inte på grund av vetskapen om denna eventuella påverkan anses påverka någon att agera på ett visst sätt, eftersom denne inte på något sätt kan förmedla vilken handling eller resultat som ska uppnås. Det psykiska sambandet brister alltså för att en tillhandahållare av Tor-noder ska anses kunna anstifta någon att begå ett brott, även om tillhandahållande av anonymitet skulle påverka vissa användares handlande.

52 Zila, Josef, *Brottsbalk (1962:700) 23 kap. 4 §*, Lexino 2012-07-01, 2.3.1.
53 Se tingsrättens resonemang i NJA 1999 s. 561.
54 RH 2015:40.
55 Med innehållsmässig korrespondens menas i denna artikel korrespondens där en person har möjlighet att utläsa ett meddelande av något slag som inte endast är tekniska data såsom källkod eller liknande.

4.4.2 MEDHJÄLP

Medhjälp innebär att medverkanspersonen psykiskt, till exempel genom råd eller uppmuntran, eller fysiskt genom att tillhandahålla hjälpmedel försöker hjälpa till att få den otillåtna gärningen till stånd. Medhjälp omfattar de fall då påverkansgraden som krävs för anstiftan inte har uppnåtts men där någon försökt underlätta en otillåten gärning.[56]

Eftersom lagtexten tar sikte på att någon försöker underlätta att ett brott utförs, omfattas både handlingar som inte underlättar utförandet och handlingar som faktiskt försvårar utförandet, så länge medverkanspersonens handlande har varit ett faktiskt försök.[57] Medverkanspersonens påverkan kan till och med vara relativt obetydligt för att det ändå ska anses som ett främjande.[58]

Gränsen för vad som räknas som ett straffbart främjande är lågt ställd vilket i förarbetena bland annat uttrycks genom formuleringen ”[…] öva inflytande på händelseutvecklingen i brottsfrämjande riktning, om så bara genom att styrka gärningsmannen i hans uppsåt.”[59]. Främjandet måste även ha skett innan eller någon gång samtidigt som gärningspersonens otillåtna gärning, men kan inte ske efter den otillåtna gärningen, varför tidpunkten för händelsen behöver klarläggas för att det ska kunna göras en bedömning.[60]

4.4.3 PSYKISKT FRÄMJANDE AV BROTT GENOM TILLHANDHÅLLANDE AV TOR-NODER

Att styrka gärningspersonen i dennes uppsåt är att betrakta som ett psykiskt främjande. Ett argument för att tillhandahållande av Tor-noder skulle innebära ett psykiskt främjande är att Tor möjliggör för personer att begå brott utan att bli identifierade och i längden straffade vilket skulle kunna anses påverka en persons benägenhet att begå brott. Det ska understrykas att det idag inte finns någon erkänd statistik eller andra uppgifter om att personer skulle bli mer benägna att begå brott via internet vid användningen av Tor.

För att det ska vara fråga om psykiskt främjande torde det enligt min uppfattning i ljuset av praxis och förarbeten krävas aktiv påverkan på ett händelseförlopp, exempelvis att någon hejar på någon vid ett slagsmål eller ger tips om hur en person lättast skadas genom ett knytnävsslag.[61]

56 Zila, *Brottsbalk (1962:700) 23 kap. 4 §,* Lexino 2012-07-01, 2.3.2.
57 Asp, Ulväng och Jareborg, s. 438.
58 Asp, Ulväng och Jareborg, s. 438.
59 SOU 1944:69, *Lagstiftning om brott mot staten och allmänheten*, s. 91.
60 Asp, Ulväng och Jareborg, s. 439.
61 SOU 1996:185, s. 189 och NJA 1984 s. 922.

Om en person som tvekar inför att begå ett brott beslutar sig för att skrida till verket på grund av att denne känner sig skyddad av anonymiteten som åtnjuts genom Tor-nätverket, innebär det de facto att en person övertygas om att begå ett brott. Genom att tillhandahålla Tor-noder skulle det kunna argumenteras för att tillhandahållarna påverkar dessa användare psykiskt att begå brott; alltså, att tillhandahållarna på något sätt ”styrker gärningspersonerna i deras uppsåt” genom att erbjuda Tor-noder. För att hållas ansvarig för medhjälp krävs dock som beskrivits att medverkanspersonens främjande rör huvudbrottet. Eftersom tillhandahållare av Tor-noder inte korresponderar med användarna, får någon information om när användarna använder deras noder eller ser vad användarnas trafik innehåller, är det svårt för tillhandahållaren att lista ut vilken gärning de ska uppmuntra genom sitt tillhandahållande. Det går inte att bara hoppas att en okänd person ska genomföra en viss handling och vidta åtgärder för att det ska ske för att hållas ansvarig för medhjälp, utan medverkanspersonen behöver åtminstone ha en uppfattning om vilken konkret gärning gärningspersonen tänker vidta.

Att bara tillhandahålla en möjlighet till anonymitet, utan att veta vilken gärning användaren har för avsikt att vidta, eller vilken typ av brott denne vill begå bör inte kunna innebära att tillhandahållaren av Tor-noder psykiskt främjar ett brott på så sätt som enligt lagen krävs för medhjälp genom psykiskt främjande.

4.4.4 FYSISKT FRÄMJANDE AV BROTT GENOM ATT TILLHANDAHÅLLA ANONYMITET

Frågan om ansvar för medhjälp i digitala miljöer har under senare år aktualiserats mer och mer,[62] och redan 1996 i den så kallade BBS-domen[63] berörde HD frågan ytligt. HD kunde dock inte pröva frågan om medverkan på grund av utformningen av åklagarens ansvarspåståenden, och HD har ännu inte prövat frågan. Däremot prövades frågan i TPB-domen där Svea hovrätt hänvisade till BBS-domen i sitt resonemang. Svea hovrätt prövade om

62 Se bl.a. Svea hovrätt, dom den 2013-10-31, mål nr B 3117-13, om medverkan till upphovsrättsbrott och Svea hovrätt, dom den 2016-03-30, mål nr B 2932-16, om medverkan till bedrägeri.
63 NJA 1996 s. 79. En tillhandahållare av BBS (Bulletin Board System) kunde åläggas ansvar för upphovsrättsbrott enligt 53 § lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk (upphovsrättslagen). På anslagstavlan laddades datorprogram upp av användare och gjordes möjliga att ladda ner för allmänheten utan att upphovspersonerna samtyckt till det. Enligt HD krävdes det med hänsyn till legalitetsprincipen att tillhandahållande av en BBS anses vara en aktiv handling för att ansvar ska kunna uppkomma för tillhandahållandet. HD ansåg att tillhandahållande av BBS i detta fall inte var en aktiv handling, trots att tillhandahållaren förutom att tillhandahålla tjänsten genom sin enhet aktivt hade genomfört viruskontroller av det som laddades upp på BBS:n, styrt om sökvägar och hade upprättat ett särskilt utrymme för vad tillhandahållaren ansåg vara kommersiellt skyddade program.

tillhandahållarna av fildelningshemsidan The Pirate Bay (”TPB”) gjort sig skyldiga till medverkan till upphovsrättsbrott enligt 53 § upphovsrättslagen.[64] I TPB-domen ansåg Svea hovrätt att TPB genom att tillhandahålla sökfunktioner, uppladdnings- och lagringsmöjligheter för torrentfiler, och trackers som förmedlade kontakter mellan enskilda fildelare underlättade huvudbrottet genom att förenkla och påskynda förverkligandet av det.[65] Svea hovrätt ansåg alltså att de funktioner som erbjöds genom TPB utgjorde en sådan tjänst som underlättade de upphovsrättsbrott som användarna utförde på hemsidan.

I ett annat mål från Svea hovrätt (”hubb-domen”)[66] angående medhjälp till upphovsrättsbrott dömdes en person för att ha tillhandahållit en så kallad DirectConnect-hubb. Genom att administrera och anordna DirectConnect-hubben kunde användare koppla upp sig mot hubben och dela filer med upphovsrättsligt skyddat material utan upphovspersonernas samtycke. Personen som tillhandahöll hubben hade enligt Svea hovrätt även haft kännedom om hur tekniken bakom fildelning fungerar och att det via den tillhandahållna hubben delades upphovsrättsligt skyddade filer utan upphovspersonernas samtycke.[67] Svea hovrätt lade här alltså vikt vid att personen hade tillhandahållit möjlighet för andra personer att begå brott genom den funktion som personen tillhandahöll. Personens vetskap om att användare utförde olagliga handlingar var även en förutsättning för ansvar enligt det allmänna skuldkravet.

Tillhandahållande av Tor-noder underlättar inte som i hubb-domen möjligheten för användarna att korrespondera med varandra och dela information av något slag. Vidare saknar tillhandahållare av Tor-noder kännedom om vilken trafik som går genom de tillhandahållna noderna, varför de saknar kännedom om vad användarna gör när de använder sig av Tor. Tor-noder skulle kunna jämföras med hubbar eftersom de båda fungerar som nav, men där slutar också likheterna mellan hubb-domen och tillhandahållandet av Tor-noder.

Tillhandahållande av Tor-noder ger inte användaren verktyg att exempelvis ladda ner upphovsrättsligt skyddat material i strid med upphovspersonens vilja eller möjlighet att ta del av barnpornografi. De som tillhandahåller verktygen för detta är de som upprättar tjänster i form av exempelvis hemsidor

64 Lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk.
65 TPB-domen, s. 24.
66 Svea hovrätt, dom den 2013-10-31, mål nr B 3117-13.
67 Hubb-domen, s. 5.

eller nedladdningsprogram för dessa syften. Att användare skulle kunna välja att utnyttja Tor när de använder dessa tjänster kan inte likställas med att de som tillhandahåller Tor-noder skulle främja användarnas handlingar eftersom tillhandahållarna av Tor-noder inte kan påverka händelseförloppet.

Användande av Tor kan inte anses förenkla eller påskynda utförandet av brott eftersom Tor-nätverket endast möjliggör anonymisering vilket inte påverkar utförandet av själva brottet. För att använda Tor-nätverket krävs dessutom en del arbete från användaren i form av att användarens enhet behöver konfigureras och en så kallad Tor-browser ska installeras och användas för att bättre säkerhet och anonymitet ska uppnås. Trafiken i Tor går dessutom långsammare än när internet används utan Tor eftersom det inte finns så många Tor-noder i nätverket som trafiken kan dirigeras genom. Detta borde betyda att användningen av Tor vid utförande av brott på internet dels komplicerar och dels saktar ner utförandet av brotten, alltså tvärtemot fallet i TPB-domen.

Även om kravet för vad som utgör främjande är lågt ställt krävs att medverkanspersonens främjandegärning är kontrollerad, vilket innebär att medverkanspersonen ska kunna avsluta eller hejda skeendet genom sin handling.[68] Hade tillhandahållare av Tor-noder behövt godkänna all trafik som går genom deras noder eller om de hade haft möjlighet att dirigera trafik till sidor med bara olagligt material hade de haft påverkan på händelseförloppet. De hade då kunnat vara medhjälpare till gärningspersoner, men så är inte fallet. Möjliggörande av anonymitet via Tor bör därför inte i sig kunna utgöra ett främjande enligt lagens mening även om identifieringen av gärningspersonen försvåras.

4.4.5 FYSISKT FRÄMJANDE AV BROTT ATT TILLHANDAHÅLLA BANDBREDD

Tillhandahållare av Tor-noder tillgängliggör som beskrivits i avsnitt 3.1.3 bandbredd samt sin IP-adress. I TPB-domen hölls en person ansvarig för att ha tillhandahållit datorskåp och bandbredd till de personer som drev TPB.[69] Eftersom tillhandahållaren i TPB-domen tillhandahöll hjälpmedel till de som drev TPB och ingen av dem var misstänkta för huvudbrottet utgjorde prövningen medhjälp till medhjälp. Svea hovrätt avgjorde dock inte frågan baserat på om handlingen i sig var ett främjande i lagens mening utan fokuserade sin prövning på tillhandahållarens uppsåt. Alltså kan det sägas att medhjälpsgärningar objektivt sett kan vara lagliga, men på grund av uppsåt utgör ett främjande av annans brottsliga gärning och är därmed straffbara. Å andra sidan är gränsen för vad som utgör främjande av brott låg vilket

68 Asp, Ulväng och Jareborg, s. 40.
69 TPB-domen, s. 30.

innebär att även småskaliga handlingar som underlättar utförande av brott kan utgöra medhjälp.

Tillhandahållandet av bandbredd i Tor innebär dels att användarnas trafik kan överföras mellan Tor-noderna och i slutändan nå målet, och dels att användarna kan dölja sig bakom tillhandahållarnas IP-adresser. Användarna av Tor-nätverket behöver dock själva ha tillgång till en internetanslutning och själva avgöra vilken hemsida de vill besöka eller vilka meddelanden de vill skicka. De användare som utför brott när de använder Tor utnyttjar tillhandahållarnas bandbredd för att utföra brottet. Även om tillhandahållarnas bandbredd inte är nödvändig för utförandet av brottet utgör den de facto ett steg i den brottsliga handlingen. Mot bakgrund av att gränsen för vad som anses utgöra ett främjande är ställd lågt bör det kunna anses att tillhandahållandet av bandbredd objektivt sett främjar en användares brottsliga gärning.

I TPB-domen klargjordes att tillhandahållandet av bandbredd möjliggjorde för tillhandahållarna av TPB att driva hemsidan.[70] Eftersom tillhandahållandet av TPB ansågs utgöra medhjälp till brott mot upphovsrättslagen då många användare av TPB begick upphovsrättsbrott främjade alltså tillhandahållaren av bandbredd i TPB-domen främjandet av ett huvudbrott. Även om tillhandahållare av Tor-noder inte på ett lika direkt sätt möjliggör för gärningspersoner att utföra brott främjar de, enligt allmänna bedömningsgrunder för medhjälp och enligt Svea hovrätts resonemang, ett huvudbrott eller ett främjande av huvudbrott eftersom tillgången till bandbredd för användaren utgör ett led i utförandet av huvudgärningen.

Detta innebär inte i sig att tillhandahållare av Tor-noder ådrar sig straffrättsligt ansvar för tillhandahållandet, utan det krävs även någon form av uppsåt eller oaktsamhet. Eftersom Svea hovrätt fäste stor vikt vid tillhandahållarnas uppsåt och vetskap om de otillåtna gärningarna som främjats, behöver tillhandahållare av Tor-noders uppsåt och vetskap beröras. Uppsåtsbedömningen vid medverkan ska göras i två led: dels huruvida medverkanspersonen haft uppsåt till sin egen handling, och dels om medverkanspersonen haft uppsåt till huvudgärningen.[71] I fråga om Tor innebär det att tillhandahållaren behöver ha uppsåt till att tillhandahållandet är ett främjande av huvudgärningen samt att huvudgärningen utförs.

Som tidigare påpekats finns ingen statistik eller bekräftade uppgifter om vad användarna av Tor gör när de utnyttjar tjänsten. Tillhandahållarna av TPB

70 TPB-domen, s. 34.
71 NJA 2003 s. 473.

hade å andra sidan vid flera tillfällen uppmärksammats på att de begick upphovsrättsintrång och mottog dessutom flertalet varningsbrev.[72] Tillhandahållarna av TPB behövde alltså inte ha någon direkt korrespondens med gärningspersonerna för att få kännedom om att det begicks brott på TPB utan det räckte med att de över huvud taget fått kännedom om användarnas gärningar. Det krävdes alltså kännedom om typen av otillåten gärning för att tillhandahållarna av TPB skulle kunna hållas ansvariga.[73] Kravet på kännedom om en vidtagen gärning kommer ur att uppsåtet måste täcka de utförda handlingarna. Det går alltså inte att ha ett generellt uppsåt till ett visst brott.[74] Svea hovrätt understryker i TPB-domen att det är tjänstens karaktär och hur användare väljer att utnyttja tjänsten som avgör om tillhandahållandet kan utgöra ett straffbart främjande.[75]

När tillhandahållarna av Tor-noder konfigurerat sina enheter och underhåller noderna med el och internetanslutning har de vetskap om att deras noder närsomhelst kan vara tillgängliga för användarna av Tor. Från och med att en tillhandahållare av Tor-noder konfigurerat sin enhet bör tillhandahållarna anses ha en kontinuerlig vilja att någon ska utnyttja noderna, men det går inte att jämställa med att tillhandahållarna av Tor-noder också skulle ha uppsåt eller kännedom om vad användarna gör när de använder Tor. Det kan därför inte anses vara vedertaget att Tor i huvudsak används för brottsliga gärningar. Tillhandahållarna kan inte heller anses ha sådan kännedom om brottslig aktivitet baserat på tjänstens karaktär eller hur användarna väljer att utnyttja den att de skulle kunna ha uppsåt till brott.

Det ska därför konstateras att tillhandahållare av Tor-noder genom tillhandahållande av bandbredd i Tor objektivt kan anses främja användares brottsliga handlingar. Däremot saknar tillhandahållarna generellt kännedom om användarnas handlingar och därmed det uppsåt som krävs för att kunna hållas ansvariga. Tjänstens karaktär eller hur användarna väljer att utnyttja tjänsten indikerar inte heller att tillhandahållarna skulle ha kännedom om att brottslig aktivitet skulle äga rum med hjälp av deras Tor-noder. I slutändan är tillhandahållarens uppsåt en bevisfråga som rätten behöver ta ställning till likt i TPB-domen. Tillhandahållare av Tor-noder bör därför inte anses kunna hållas ansvariga för medhjälp.

72 TPB-domen, s. 25.
73 TPB-domen, s. 41.
74 TPB-domen, s. 27.
75 TPB-domen, s. 23 f.

4.4.6 OAKTSAM MEDVERKAN

För att oaktsam medverkan ska vara straffbar krävs att även oaktsamhet enligt huvudbrottet är straffbart.[76] Det finns flera brott, bland annat vissa former av barnpornografibrott och upphovsrättsbrott, där oaktsamhet eller grov oaktsamhet räcker för att hållas ansvarig. Det finns två typer av oaktsamhet som båda kan leda till ansvar: medveten oaktsamhet och omedveten oaktsamhet.

I stora drag innebär medveten oaktsamhet för tillhandahållare av Tor-noder att denne skulle uppfatta att det är sannolikt att en viss huvudgärning inträffar om Tor-noderna tillhandahålls och att tillhandahållaren är likgiltig inför risken att denna huvudgärning inträffar. Omedveten oaktsamhet innebär istället att tillhandahållaren haft skälig anledning att anta eller borde ha förstått att en viss huvudgärning skulle inträffa, men inte gjorde det vid tillhandahållandet av Tor-noderna.

Båda dessa fall kräver alltså att tillhandahållaren ska ha någon form av uppfattning – eller borde ha någon form av uppfattning – om vad användarna gör när de använder Tor. Eftersom tillhandahållarna av Tor-noder inte har någon kännedom om vad användarna gör när de använder Tor är medveten oaktsamhet därför utesluten.

Frågan om omedveten oaktsam medverkan blir mer intressant eftersom det inte ställs krav på att medverkanspersonen förstått att en viss huvudgärning kunde inträffa. Ett exempel på omedveten oaktsamhet framgår av ett avgörande från HD då en revisor hölls ansvarig för medhjälp till bokföringsbrott genom grov oaktsamhet då denne noterat att boksluten för ett bolag hade inneburit ovanligt stora arbetsinsatser för kollegorna som arbetade med ärandet, men underlåtit att kontrollera saken närmare.[77]

Bedömningen av omedveten oaktsamhet ska inledas med frågan om tillhandahållare av Tor-noder kan göra något för att komma till insikt om hur deras noder används. Det kan handla om att vara uppmärksam, inhämta information eller skaffa hjälp för att hitta information. Tillhandahållare av Tor-noder har viss möjlighet att få reda på vilken trafik som överförs genom noden. För att kunna ta reda på detta krävs ett omfattande arbete som bland annat kan innebära att konfigurera skadliga Tor-noder. Det är svårt och krångligt att vidta sådana åtgärder eftersom Tor är uppbyggt för att det inte ska gå att spåra trafiken. Av de internet-sökningar och intervjuer som gjorts, av

76 SOU 1944:69, s. 94.
77 NJA 1988 s. 383.

mig med personer som är engagerade i och är med och utvecklar Tor, framgår att ingen har fullständig kännedom om hur detta görs och ingen vill heller försöka eftersom detta skulle påverka Tor-nätverket negativt.

Nästa fråga är om tillhandahållaren haft möjlighet att vidta de åtgärder som skulle krävas för att få kännedom om trafiken i Tor-noderna. Med tanke på hur svårt det verkar vara att få information om trafiken i Tor-nätverket måste det konstateras att tillhandahållare har en liten möjlighet att vidta de åtgärder som skulle behövas. Även om bedömningen av tillhandahållarens möjlighet ska göras baserat på den enskilda tillhandahållarens tekniska kunskap måste det anses som att väldigt få tillhandahållare har möjlighet att vidta sådana åtgärder.

Den slutliga frågan är om det är rimligt att samtliga tillhandahållare av Tor-noder skulle vidta de åtgärder som krävs för att få information om trafiken i Tor-noderna. Som redan betonats i den första frågan är det väldigt svårt att ta reda på denna information och det krävs omfattande teknisk kunskap samt resurser för att åstadkomma den insikt som krävs. Det kan därför inte anses vara rimligt att samtliga tillhandahållare av Tor-noder vidtar de möjliga åtgärderna för att få insikt om vilken trafik som går genom noderna.

Med tanke på att tillhandahållarna av Tor-noder inte endast möjliggör anonymitet till de användare som väljer att begå brott när de använder Tor samt att antalet användare som begår brott inte kan avgöras, bör det anses orimligt för samtliga tillhandahållare av Tor-noder att vidta sådana åtgärder för att komma till insikt om att en eventuell huvudgärning kan komma att utföras när deras noder används.

Orimligheten bör alltså dels anses ligga i att det idag inte finns några konkreta indikationer på att det skulle begås många brott av de som använder Tor, och dels att åtgärderna är oproportionerliga i förhållande till den insats som tillhandahållarna skulle behöva göra för att få reda på information om var trafiken genom deras noder går.

Det ska här också tilläggas att det i princip är tekniskt omöjligt att identifiera exakt vilken IP-adress trafiken kommer ifrån och vart den går från noderna. Det är i nästa led ännu svårare att ta reda på om det faktiskt finns en fysisk person bakom IP-adressen.

4.5 SOCIAL ADEKVANS

Innan uppsåt eller oaktsamhet prövas ska frågan om det föreligger några rättfärdigande omständigheter prövas. Frågor om rättfärdigande omständigheter

presenteras här, efter redogörelsen för uppsåts- och oaktsamhetsbedömningen, i syfte att presentera en tydligare redogörelse av den straffrättsliga bedömningen av Tor-noder för det fall att några rättfärdigande omständigheter inte skulle föreligga.

Det kan inte anses föreligga nödvärn, nöd eller samtycke vid döljandet av någons identitet genom tillhandahållandet av Tor-noder om användaren begår brott; däremot skulle tillhandahållandet kunna vara socialt adekvat. I TPB-domen berördes frågan om tillhandahållandet av TPB kunde anses vara tillåten på grund av social adekvans.

Svea hovrätt klargjorde i TPB-domen att en gärning som innefattar ett medvetet risktagande i förhållande till ett skadligt resultat under vissa förutsättningar kan vara tillåten med beaktande av omständigheter såsom: typen av risk, vilka värden riskerna riktar sig mot, själva gärningens sociala värde samt vilka försiktighetsåtgärder som varit möjliga och befogade att vidta.[78] Bedömningen ska enligt hovrättens resonemang alltså göras utifrån om tillhandahållande av Tor-noder kan anses vara tillräckligt värdefullt eller viktigt i allmänhet, samtidigt som de oönskade riskerna är proportionerliga i förhållande till värdet av tjänsten. Svea hovrätt nämnde exempelvis utan att närmare gå in på någon redogörelse att Google och YouTube brukar ges som exempel på hemsidor som i allmänhet uppfattas som legitima även om det ibland förekommer att det exempelvis laddas upp material som utgör upphovsrättsintrång.[79]

I fallet med TPB konstaterade Svea hovrätt att tjänsten till övervägande del utnyttjats för fildelning av musik, film och spel men att det inte gick att klarlägga hur stor del av materialet som var uppladdat med upphovspersonens samtycke. Av vittnesmål framgick dock att det mesta eller till och med ”kopiösa” mängder av det som fanns på TPB var upphovsrättsligt skyddat material som uppladdats utan upphovspersonernas samtycke. Det åberopades även varningsbrev och liknande som tillhandahållarna av TPB hade mottagit angående att det på TPB fanns material som utgjorde upphovsrättsintrång, men som tillhandahållarna inte agerat på eller vidtagit några åtgärder att förändra. Baserat på detta konstaterade Svea hovrätt slutligen att social adekvans inte förelåg eftersom

78 TPB-domen, s. 24: ”Om en söktjänst till sin karaktär är sådan att den i första hand är ett värdefullt verktyg i laglig verksamhet och allmänt samhällsnyttig, om denna legitima användning dominerar, men spridning eller överföring av olagligt material trots försiktighetsåtgärder inte kan uteslutas, kan driften av en sådan tjänst i objektivt hänseende komma att bedömas som tillåten med stöd av nyss nämnda teorier.”

79 TPB-domen, s. 24.

det legitima intresset att sprida material med upphovspersoners samtycke via TPB inte uppvägdes av den uppenbara risk för upphovsrättsintrång för flera andra upphovspersoner då verksamheten bedrivits i så massiv omfattning.[80] I fråga om tillhandahållande av Tor-noder finns det i dag ingen statistik på hur många av användarna som begår brott när de använder sig av Tor. Det är inte heller troligt att denna information inom en snar framtid kommer kunna gå att kartlägga på grund av Tor-nätverkets tekniska konstruktion. Det är därför svårt att föra ett djuplodande resonemang i denna del.

Det finns inget i konstruktionen av Tor-nätverket som indikerar att nätverket är uppbyggt i syfte att främja brott eller dölja brottslingar. Det framgår inte heller av presentationen av Tor att nätverket skulle vara riktat till personer som vill dölja sin brottslighet, tvärtom marknadsförs Tor som ett sätt att stärka skyddet för personers integritet och yttrandefrihet. Dessa värden får anses vara av stor vikt och i ett demokratiskt samhälle och är även uttryckligen grundlagsskyddade både nationellt och genom EU:s rättighetsstadga.[81] Det torde därför kunna anses vara socialt adekvat att tillhandahålla Tor-noder trots att det i vissa fall skulle kunna försvåra eller dölja gärningspersoners identitet. Det bör därför kunna anses föreligga rättfärdigande omständigheter som gör det tillåtet att tillhandahålla Tor-noder trots att användare kan använda nätverket för att begå brott.

5. SUMMERING OCH AVSLUTANDE ORD

Denna betraktelse har givit en överblick över några av de straffrättsliga frågor som aktualiseras vid tillhandahållande av Tor-noder. Samtliga slutsatser i redogörelsen har givit att den tekniska konstruktionen av Tor-nätverket leder till att tillhandahållaren inte bör kunna hållas straffrättsligt ansvarig för tillhandahållandet av Tor-noder.

Tillhandahållandet av Tor-noder bör i sig inte kunna anses utgöra något brott eftersom det saknas brottsbeskrivningsenlighet med något huvudbrott som idag är lagstadgat. Genom att tillhandahållare av Tor-noder saknar insyn i den trafik som överförs via Tor-noder, och svårligen kan komma att få sådan insyn på grund av Tor-nätverkets tekniska konstruktion, bör tillhandahållare inte heller kunna åläggas ansvar för medverkan då de saknar uppsåt och inte heller kan anses agera oaktsamt vid tillhandahållandet. Om det likväl skulle bedömas utgöra en otillåten gärning eller medverkan till sådan, bör det finnas möjlighet att tillämpa den rättfärdigande omständigheten social adekvans eftersom det genom

80 TPB-domen, s. 25.

81 Sv. Europeiska unionens stadga om de grundläggande rättigheterna (2010/C 83/02)SV 30.3.2010 Europeiska unionens officiella tidning C 83/389, artikel 7 och 11.

konstruktionen av Tor-nätverket inte finns något som indikerar att nätverket är uppbyggt i syfte att främja brottsliga aktiviteter och det idag inte heller finns några bekräftade uppgifter om att Tor främst skulle användas för brottslig aktivitet.

Med detta sagt återstår det att se hur Tor och liknande tjänster kommer bedömas av domstolarna. Flera frågor återstår att utreda för domstolarna och ett klart svar kan endast ges från fall till fall. För att kunna ge en fullständig bild av hur Tor-noder skulle kunna komma att bedömas av domstolar skulle det krävas en omfattande fortsatt utredning av frågorna och sannolikt kan inga säkra svar ges förrän domstolarna har fått säga sitt.