Tillhandahållande av Tor-noder – rättsliga aspekter

Paulina Rehbinder

2016-11-07

it girl law

JOURNALIST FÖRBUNDET

Innehållsförteckning

Förkortningar

BrB	Brottsbalk (1962:700)
HD	Högsta domstolen
ISP	Internet Service Provider (internetleverantör)
LEK	Lag (2003:389) om elektronisk kommunikation
RB	Rättegångsbalk (1942:740)
TPB	The Pirate Bay (hemsida för fildelning)

Sammanfattning

Denna rapport ger en översiktlig bild av rättsläget vid tillhandahållande av Tor-noder. Analysen är begränsad till rättsläget i Sverige och utgångspunkten är att samtliga användare, tillhandahållare och Tor-noder befinner sig i Sverige.

Rapporten tar avstamp i frågan om den som tillhandahåller en Tor-nod tillhandahåller ett allmänt elektroniskt kommunikationsnät eller tjänst som är anmälningspliktig till Post- och telestyrelsen (PTS). Frågan är viktig eftersom anmälningsplikt bland annat innebär en skyldighet att lagra information om användarnas användning av tjänsten.

Slutsatsen i denna del är att anmälningsplikt och datalagringsskyldighet inte bör anses föreligga. Det skäl som redogörs i denna rapport är att Tor-noder inte tillhandahålls för kommersiellt bruk eller mot ersättning vilket är ett krav enligt lag för att anmälningsplikt ska aktualiseras.

Rapportens andra del fokuserar på straffrättsligt ansvar för tillhandahållare av Tor-noder. Vid en genomgång av straffrätten går det inte att hitta någon brottsbeskrivning som direkt stämmer överens med tillhandahållandet. Trots detta görs en genomgång av de två mest närliggande brottsbeskrivningarna.

- Skyddande av brottsling:
    - Det krävs att någon eller någons brottsliga gärning döljs efter att ett brott blivit begånget för att kunna hållas ansvarig för skyddande av brottsling.
    - Eftersom tillhandahållare av Tor-noder möjliggör anonymitet under tiden en användare eventuellt utför ett brott utgör tillhandahållandet inte något skydd för brottslingen efter det att brottet begåtts varför tillhandahållare inte bör anses skydda brottslingar i lagens mening.
- Uppvigling:
    - Det krävs enligt brottsbeskrivningen någon form av meddelande om vilken brottslig gärning som ska utföras för att hållas ansvarig.
    - Eftersom det inte sker någon innehållsmässig korrespondens mellan tillhandahållare och användare av Tor bör tillhandahållandet inte i sig inte utgöra någon uppvigling.

Tillhandahållares eventuella ansvar för medverkan till någon användares brott genom att endast tillhandahålla Tor-noder behandlas också i rapporten. Medverkan kan ske både psykiskt och fysiskt varför olika former av medverkan behandlas i rapporten.

- Anstiftan:
    - Utgör ett psykiskt främjande där anstiftaren förmår någon annan att begå ett brott exempelvis genom att uppdra någon att utföra brottet.
    - Tillhandahållare av Tor-noder bör inte kunna hållas ansvariga för anstiftan till användares brott enbart baserat på själva tillhandahållandet av Tor-noderna eftersom det saknas innehållsmässig korrespondens mellan tillhandahållare av Tor-noder och användare vilket är ett krav för att kunna påverka någon psykiskt.
- Psykisk medhjälp:
    - Innebär att någon psykiskt påverkar någon utförande av brott, exempelvis genom att ge råd till någon om hur ett brott ska utföras.
    - Likt anstiftan saknas innehållsmässig korrespondens mellan tillhandahållare av Tor-noder och användare vilket krävs för att kunna påverka någon psykiskt. Tillhandahållare av Tor-noder bör därför inte kunna hållas ansvariga för medhjälp till användares brott enbart baserat på själva tillhandahållandet av Tor-noderna.
- Fysisk medhjälp genom tillhandahållande av anonymitet:
    - Tillhandahållande av anonymitet genom Tor bör i sig inte anses främja en användares eventuella brott eftersom det inte påverkar utförandet av brottet.
    - Tillhandahållare av Tor-noder saknar vetskap om vad användarna gör när de utnyttjar Tor-noderna och det är svårt för tillhandahållare ta reda på detta. Detta innebär att tillhandahållare inte bör kunna anses ha uppsåt till användarnas brott vilket krävs för att kunna hållas ansvarig för medverkansbrott.

- Fysisk medhjälp genom tillhandahållande av bandbredd:
    - Tillhandahållandet av bandbredd genom Tor-noder kan komma att utgöra ett främjande av brott eftersom det möjliggör att trafiken överförs till slutdestinationen.
    - Tillhandahållare av Tor-noder saknar dock vetskap om vad användarna gör när de utnyttjar Tor-noderna och det är svårt för tillhandahållare ta reda på det. Detta innebär att tillhandahållare inte bör kunna anses ha uppsåt till användarnas brott vilket krävs för att kunna hållas ansvarig för medverkansbrott.

Skulle en tillhandahållare få kännedom om att ett brott pågår och att deras noder används för det skulle dock tillhandahållaren eventuellt kunna hållas ansvarig om denne har möjlighet att stänga av noden men medvetet väljer att inte gör det i syfte att brottet ska fullbordas eller fortgå. För medverkan till vissa brott behövs bara oaktsamhet istället för uppsåt. Även i dessa fall ställs det krav på att tillhandahållaren ska ha vetskap om att ett brott begås varför samma förutsättningar saknas som vid bedömningen av uppsåt.

I rapporten berörs också situationen då en tillhandahållare anses utföra eller medverka till brott men där regler för ansvarsfrihet enligt social adekvans, eller straffrihet enligt e-handelslagen och straffnedsättning enligt brottsbalken, bör kunna tillämpas.

Vidare behandlas frågor gällande ansvar för och inom juridiska personer i rapporten. De juridiska personer som tillhandahåller Tor-noder bör kunna påföras företagsbot i det fall tillhandahållande av Tor-noder skulle anses utgöra brott eller medverkan till brott. Den person som i den juridiska personen anses ansvara för tillhandahållandet av Tor-noden bör bedömmas likt andra tillhandahållare.

I den tredje och avslutande delen av rapporten behandlas bland annat anknytande frågor om tvångsmedel oaktat tillhandahållarnas eventuella straffrättsliga ansvar.

De tvångsmedel som behandlas i rapporten är:

- Beslag:
    - Kan göras även hos en annan person än den som misstänks för brottet om resultatet av beslaget bedöms kunna underlätta utredning av brottet.
    - Ingreppet behöver vara proportionerligt i förhållande till vad som kan inhämtas genom beslaget.
    - Eftersom en Tor-nod inte lagrar någon information, mer än nodens krypteringsnycklar, kan ett beslag av Tor-noder anses vara oproportionerligt i förhållande till ingreppet. Därför bör beslag av Tor-noder i sig inte anses vara tillåtet. Skulle en enhet användas för andra ändamål utöver att verka som Tor-nod kan det vara proportionerligt att beslagta enheten, men detta beror då på andra anledningar än tillhandahållandet av Tor-noder.
- Husrannsakan:
    - Rättsvårdande myndigheter ges tillstånd att ta sig in i hus, rum och andra förvaringsställen vilket kan användas i syfte att beslagta föremål. Detta skulle troligtvis vara fallet med Tor-noder.
    - Husrannsakan behöver vara proportionerligt i förhållande till resultatet av ingreppet.
    - Det är i dagsläget oklart om tillstånd för husrannsakan även krävs för att ta del av information på exempelvis hårddiskar eller om detta är tillräckligt. Det pågår dock en utredning gällande förutsättningar för att kunna utföra husrannsakan på distans där denna fråga ska utredas.
    - Husrannsakan för att beslagta Tor-noder bör idag kunna anses vara oproportionerligt eftersom det inte lagras någon annan information i noderna än nodernas krypteringsnycklar. Därför bör husrannsakan för att beslagta Tor-noder i sig inte kunna anses vara tillåtet.

- Hemlig avlyssning och övervakning av elektronisk kommunikation:
    - Utgör en möjlighet för rättsvårdande myndigheter att i hemlighet kunna ta del av meddelanden som överförs via elektroniska kommunikationsnät exempelvis e-post. Detta är ett undantag från huvudregeln att detta är förbjudet och även kan innebära ett brott.
    - Endast de som omfattas av vissa bestämmelser i lagen om elektronisk kommunikation ska möjliggöra hemlig avlyssning och övervakning. Eftersom tillhandahållare av Tor-noder inte ska anses omfattas av lagen ska de inte heller möjliggöra hemlig avlyssning och övervakning av sina Tor-noder.

Det pågår för närvarande även en utredning om möjligheten till hemlig dataavläsning. Resultaten av de pågående utredningarna kan komma att påverka möjligheten för rättsvårdande myndigheter att få insyn i trafik som överförs i Tor-nätverket. Detta kan leda till att den anonymitet och skydd som Tor-nätverket medger försvagas och medför risk för att exempelvis källskyddet olovligen bryts.

Sammanfattningsvis bör i dagsläget tillhandahållare av Tor-noder inte anses kunna bli ansvariga för tillhandahållande av Tor-noder enligt de regler som berörs i rapporten både gällande anmälningsplikt och straffrättsliga bestämmelser. Däremot kan ansvar baserat på konsumenträtt och liknande aktualiseras.

Det ska dock påminnas om att tillhandahållande av Tor-noder ännu inte prövats av domstol i Sverige varför framtiden får utvisa hur frågorna kommer att bedömas i praktiken.

Abstract

This report gives an overview of the legal situation in the provision of Tor nodes. The analysis is limited to the legal situation in Sweden, and the starting point is that all users, suppliers and Tor nodes are located in Sweden.

In the first part of the report the question of whether a provider of Tor nodes is providing a public electronic communications network or service is examined, which is notifiable to the Swedish Post and Telecom Authority (PTS). The question is important, because the notification requirement involves an obligation to store information about the users' usage of the service.

The conclusion in this part is that there should be no obligation to notify or store data. The reason set out in this report is that Tor nodes are not supplied for commercial use or for remuneration, which is a requirement by law in order for the obligation of notification to arise.

The second part of the report focuses on criminal liability for suppliers of Tor nodes. In a review of criminal law, it is not possible to find any offenses which directly correspond with the provision of Tor nodes. However, the two most related offenses are reviewed in the report.

- Protection of a criminal:
    - In order to be held responsible for protecting a criminal, it is required that someone or someone's criminal offense is hidden after a crime has been committed.
    - Since providing Tor nodes makes anonymity possible during the time a user may perform a crime, the provision does not constitute any protection for the criminal after the crime was committed, which is why suppliers should not be considered to protect criminals in the meaning of the law.

- Incitement:
    - According to the description of the offense, in order to be held responsible, there is a requirement for some form of communication about the criminal act that should be performed.
    - Since there is no content-based correspondence between suppliers and users of Tor, the provision in itself should not constitute any incitement.

A supplier's possible liability for participation in any user's crime by only providing Tor nodes is also dealt with in the report. Participation may take place both psychologically and physically, which is why different forms of participation are dealt with in the report.

- Instigation:
    - Constitutes a psychological promotion where the instigator is able to get another person to commit a crime, for example, by instructing someone to carry out the crime.
    - Suppliers of Tor nodes should not be held responsible for the instigation of crimes committed by users that are only based on the provision alone of Tor nodes, as there is no content-based correspondence between the suppliers of Tor nodes and users, which is a requirement in order to influence anyone psychologically.
- Psychological assistance:
    - Means that someone psychologically prompts some execution of an offense, for instance by giving advice to someone about how a crime should be carried out.
    - Like instigation, there is no content-based correspondence between suppliers of Tor nodes and users which is required in order to be able to prompt someone psychologically. Suppliers of Tor nodes should therefore not be able to be held liable for aiding users' offenses based only on the actual provision of the Tor nodes.

- Physical assistance through the provision of anonymity:
    - The provision of anonymity through Tor should not in itself be considered to promote a user's possible offense, because it does not affect the execution of the offense.
    - Suppliers of Tor nodes do not have knowledge of what the users do when they use the Tor nodes, and it is difficult for suppliers to ascertain this. This means that suppliers should not be considered to be able to have the intent to the users' offenses which is required to be able to be held responsible for the participation in the offense, merely based on the provision of Tor nodes.
- Physical assistance through the provision of bandwidth:
    - The provision of bandwidth through Tor nodes may constitute an assistance of offenses, because it allows the traffic to be transferred to the final destination.
    - However, suppliers of Tor nodes do not have knowledge of what the users do when they make use of the Tor nodes, and it is difficult for suppliers to ascertain this. This means that suppliers should not be considered to be able to have the intent to the users' offenses which is required to be able to be held responsible for the participation in the offense, merely based on the provision of Tor nodes.

If a supplier becomes aware that an offense is in progress and that their nodes are used for it, the supplier should, however, in some cases be able to be held responsible if the supplier has the possibility of turning off the node, but deliberately chooses not to in order for the offense to be completed or continue. For participation in certain offenses, only negligence is needed instead of intent. Even in these cases, there is a requirement that the supplier must have knowledge that an offense is committed which is why the same conditions are missing as in the assessment of intent.

The report also deals with the situation where a supplier is considered to execute or contribute to an offense, but where rules for discharge under social adequacy (social adekvans) or impunity under the e-commerce act and reduced penalties under the Criminal Code could be applicable.

Furthermore, issues relating to responsibility for and within legal persons are dealt with in the report. The legal persons that provision Tor nodes should be able to be given corporate fines in the event that the provision of Tor nodes could be regarded as criminal offenses or participation in crime. The person who in the legal entity is considered to be responsible for the provision of the Tor node should be assessed like other suppliers.

The third and final part of the report deals with related questions about the use of coercion notwithstanding the possible criminal liability of the suppliers.

The coercive measures which are dealt with in the report are:

- Confiscation:
    - Can also be conducted at a person other than the person who is suspected of the offense if the confiscation is deemed to assist in the investigation of the offense.
    - The operation needs to be proportionate in relation to what can be obtained through the confiscation.
    - Since a Tor node does not store any information in addition to the encryption keys of the node, a confiscation of Tor nodes should be deemed to be disproportionate in relation to the operation. Therefore, the confiscation of Tor nodes in itself should not be considered to be allowed. If a device is used for other purposes than as a Tor node, confiscating the device could be proportionate, but is then depending on other reasons than the provision of Tor nodes.

- Search:
    - Judicial authorities will be given permission to enter a house, room and other storage locations which can be used for the purpose of confiscating objects. This would probably be the case with Tor nodes.
    - A search needs to be proportionate in relation to the results of the operation.
    - At the present, it is unclear whether the authorisation for searches is also needed to access information on for example hard drives. However, a governmental commission of inquiry is at the moment examining the conditions for permitting searches on a distance where this issue is to be addressed.
    - Searches to seize Tor nodes should currently be considered disproportionate, because no other information is stored in the nodes than the encryption keys of the nodes. Therefore, a search to confiscate Tor nodes in itself should not considered to be allowed.
- Secret wire-tapping and monitoring of electronic communication:
    - Constitutes an possibility for law enforcement to secretly take notice of messages transmitted by electronic communications networks such as email. This is an exemption from the general rule that this is prohibited and may also involve an offense.
    - Only the providers who fall within certain provisions in the Electronic Communications Act shall make secret wire-tapping and monitoring possible to law enforcement. Since providers of Tor nodes should not be considered to fall within the scope of the Electronic Communications Act, nor should they make secret wire-tapping and monitoring of their Tor nodes possible.

There is currently also a governmental commission of inquiry examining the possibility of "secret data readout". The results of the ongoing inquiry may affect the ability of law enforcement to gain insight into traffic that is transferred into the Tor network. The result of this could be that the anonymity and protection which the Tor network provides is weakened and results in the risk that the protection of a source for instance, is illegally broken.

In conclusion, suppliers of Tor nodes should currently not be considered to be able to be responsible for the provision of Tor nodes in accordance with the rules that are referred to in

the report both regarding to the obligation of notification and criminal liability. On the other hand, responsibility based on consumer rights and similar could arise.

However, it should be noted that the provision of Tor nodes has not yet been examined by the courts in Sweden, which is why the future will tell how the questions will be assessed in practice.

Inledning

Tor[1] är en anonymiseringstjänst som möjliggör att användare kan surfa på internet utan att trafiken till och från användares datorer kan spåras direkt till den ip-adress som användaren har. Anonymiteten i Tor uppnås genom att trafiken krypteras och överförs via så kallade Tor-noder vars ip-adresser nyttjas och anonymitet möjliggörs. Tekniken bakom Tor-nätverket kommer att beröras mer utförligt senare i rapporten.

För att nätverket ska kunna fungera krävs att det tillhandahålls så kallade Tor-noder som bildar nätverket. Desto 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 Tor-nod och idag är det både privatpersoner och juridiska personer som tillhandahåller Tor-noder.

Redan år 2012 uttryckte Journalistförbundets yttrandefrihetsgrupp[2] en önskan om att börja driva Tor-noder, men ville först utreda vilka risker som fanns kopplade till driften innan den inleddes. Journalister har en grundlagsfäst plikt att skydda sina källor. Det anges i tryckfrihetsförordningen[3] och yttrandefrihetsgrundlagen[4]. Därför är det inte bara ett intresse utan även en skyldighet för journalister att hålla kommunikationen med källor och andra journalister skyddad från insyn.[5] Vikten av att upprätthålla anonymitet för källor och andra journalister är särskilt viktig i de länder där internet är hårt övervakat av staten.[6] I vissa av dessa länder kan anonymiteten vara en fråga om liv eller död.[7] Frågan om 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.[8]

Yttrandefrihetsgruppens intresse av att kunna driva Tor-noder är således förenat med en skyldighet att bevara yttrandefriheten, inte bara i Sverige utan även globalt. Det saknas även kom-

[1] Officiell hemsida för Tor, https://www.torproject.org/.
[2] Trehörning, Pär, Officiell presentation av yttrandefrihetsgruppen, redigerad den 8 januari 2015, https://www.sjf.se/yrkesfragor/yttrande-tryckfrihet/yttrandefrihetsgruppen.
[3] Tryckfrihetsförordning (SFS 1949:105) 3:3.
[4] Yttrandefrihetsgrundlag (SFS1991:1469) 2:3.
[5] Edström, Martin och Fridh Kleberg, Carl, Anonymitet och kryptering–tips till journalister, s. 1, https://www.iis.se/docs/Anonymitet-och-kryptering-%E2%80%93-tips-till-journalister.pdf.
[6] Andersson Sus, Laurin Fredrik och Jankov Petra, Digitalt källskydd – en introduktion, s. 53, https://www.iis.se/docs/digitalt-kallskydd-2.pdf.
[7] Andersson m.fl., s. 21.
[8] MacAskill Ewen och Ackerman Spencer, NSA collecting phone records of millions of Verizon customers daily, The Guardian, den 6 juni år 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

mersiellt intresse från yttrandefrihetsgruppen att driva Tor-noder eftersom Tor ”bygger på frivilliga insatser där man delar med sig av sin kapacitet”.[9]

Det finns flera typer av användare av Tor varav några 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 skydd sina källor och militären samt rättsvårdande myndigheter som behöver skydda sin kommunikation och i vissa fall informationsinhämtande på internet.[10]

Det gemensamma intresset för samtliga användare kan sägas vara att skydda sina aktiviteter på internet från insyn. Skälen för detta kan som ovan beskrivits vara väldigt olika.

Möjligheten till anonymitet har dock kommit att skapa bekymmer hos vissa aktörer. Dessa aktörer har främst varit rättsvårdande myndigheter. Deras främsta intresse är att kunna utreda och beivra brott och därför har de ett starkt intresse av att kunna följa från vem trafik går till olika hemsidor med olagligt innehåll eller hemsidor där olagliga handlingar kan vidtas eller få insyn i meddelanden som har olagligt innehåll. Genom att använda Tor kan den som vill besöka sådana hemsidor göra detta utan att trafiken kan spåras till dennes ip-adress vilket försvårar rättsvårdande myndigheters möjligheter att utreda och beivra brott.[11] Idag 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.[12]

Det ställs krav på att tillhandahållare av allmänt tillgängliga elektroniska kommunikationsnät och allmänna elektroniska kommunikationstjänster anmäler sin verksamhet till Post- och telestyrelsen. Den som är anmälningspliktig är även skyldig att lagra viss information om sina användare och deras förehavanden på internet, så kallad datalagring. Därför är det avgörande att ta reda på om tillhandahållande av Tor-noder i Sverige leder till anmälningsplikt.

---

[9] Andersson m.fl., s. 54.
[10] Officiell hemsida för Tor, https://www.torproject.org/.
[11] Det är ännu inte klarlagt om någon har lyckats hacka Tor, men flera rykten florerar om att FBI ska ha lyckats. Ännu har inget av dessa rykten bekräftats av Tor-projektet. Se följande artiklar om frågan: Pouls, Kevin, *The FBI Used the Web's Favorite Hacking Tool to Unmask Tor Users*, Wired, den 16 december år 2014, http://www.wired.com/2014/12/fbi-metasploit-tor/, Paganini, Pierluigi, *Who hacked a cluster of Tor servers in the Netherlands?*, blog Security affairs, den 24 december 2014, http://securityaffairs.co/wordpress/31429/hacking/who-hacked-a-cluster-tor-servers.html och Carr Paul, *If you still trust Tor to keep you safe, you're out of your damn mind*, Panodaily, den 26 december år 2014, http://pando.com/2014/12/26/if-you-still-trust-tor-to-keep-you-safe-youre-out-of-your-damn-mind/.
[12] It-relaterade brott - polisens arbete, senast uppdaterad den 8 december år 2014 kl. 15:54, https://polisen.se/Om-polisen/Olika-typer-av-brott/IT-brott/.

I det fall att någon användare använder 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 besök en hemsida med barnpornografi. Det är därför viktigt att ta reda på om och 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 begått själva brottet.

Det är dessutom av yttersta vikt att skyddad information såsom källor och liknande inte blir allmänt känt vilket skulle kunna inträffa om rättsvårdande myndigheter exempelvis beslagtar en Tor-nod som även används inom journalistiskt arbete. Det ska därför i denna rapport redogöras för vilka risker det finns för att tvångsmedel kan användas mot tillhandahållare av Tor-noder och vilka typer av tvångsmedel det kan röra sig om.

I utarbetandet av denna rapport har det hållits två referensgruppsmöten med en grupp bestående av representanter från bland annat Bahnhof, Föreningen för Digitala Fri- och Rättigheter (DFRI), Myndigheten för samhällsskydd och beredskap (MSB), Polisen, Polisförbundet, SIDA, Säkerhetspolisen, TCO, forskare från flera universitet samt representanter från ett antal fackförbund. Referensgruppsmötena har syftat till att kommentera de slutsatser som dragits och ge rapporten perspektiv från den praktiska verkligheten från respektive representant. På detta sätt har rapporten i största möjliga utsträckning utformats efter de faktiska förutsättningarna i samhället idag.

Denna rapport kommer inte beröra eventuella tekniska frågor gällande Tor-nätverkets kapacitet eller förmåga. Det finns flera säkerhetsmässiga aspekter gällande Tor-nätverket som kritiserats främst gällande den faktiska anonymiteten som nätverket erbjuder. Det kommer i rapporten inte tas ställning till om Tor är detta bra verktyg för anonymitet eller den tekniska kritik som riktats mot Tor. Rapporten fokuserar därför bara på de juridiska frågeställningarna förknippade med tillhandahållande av Tor-noder. Syftet är att klargöra juridiska aspekter av tillhandahållande av Tor-noder.

Rapporten är uppdelad i tre delar. Den första delen fokuserar på frågan om tillhandahållande av Tor-noder kan leda till anmälningsplikt till Post- och telestyrelsen och i förlängningen till att tillhandahållaren måste lagra data om användarna. För att klargöra detta ska det göras en bedömning av om tillhandahållande av Tor-noder kan anses innebära tillhandahållande av

allmänt tillgängligt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst.

Den andra delen fokuserar på eventuella straffrättsliga konsekvenser av ett tillhandahållande av Tor-noder, både gällande straffansvar för huvudbrott och också medverkan till någon användares brott. Frågan om ansvar inom juridiska personer som tillhandahåller Tor-noder kommer även att beröras.

Den tredje delen berör frågor om tvångsmedel och syftar främst till att avgöra vilka praktiska sätt det finns för aktörer som hanterar känslig information att skydda informationen från att bli publik. Den tredje delen avslutas med en kortare internationell utblick där personer som är aktiva inom utvecklingen av Tor har frågats om sina erfarenheter.

Denna rapport vänder sig till privatpersoner och juridiska personer som är intresserade av att tillhandahålla Tor-noder och på förhand vill veta vilka juridiska risker och ansvar det kan finnas med att tillhandahålla Tor-noder. Detta innebär dock inte att denna rapport går att tillämpa som juridisk rådgivning i enskilda fall.

Läsaren förväntas inte att ha någon specifik kunskap om IT, teknik eller juridik, men förväntas ha en allmän kännedom om internet, samhällsfunktioner och rättssystemet i stort.

Tor och brottslig verksamhet

Tor förknippas av allmänheten många gånger med brottslig verksamhet på internet och begrepp som ”Deep web”[13] och ”Darknet”[14] 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. Stora delar av ”Deep web” består av precis samma typ av innehåll som det indexerade-internet, alltså hemsidor med bilder, text och liknande. Att material och hemsidor finns på ”Deep web” är inte heller alltid ett val som avsändaren har gör utan det kan bero på tekniska skäl som gör att sökmotorerna inte indexerar alla filtyper och liknande som läggs upp. Innehållet blir då endast tillgängligt om hela adressen skrivs in i adressfältet i webläsaren.

Vid sökningar på internet förekommer det ett antal sökträffar där användning av Tor rekommenderas för användare som vill få tillgång till material på ”Deep web”.

[13] Wikipedia om Deep web, senast besökt 2016-10-22, https://sv.wikipedia.org/wiki/Deep_web.
[14] Wikipedia om Darknet, senast besökt 2016-10-22, https://sv.wikipedia.org/wiki/Darknet.

Rekommendationerna ges i flera fall för att skydda användare mot att bli föremål för brottsliga gärningar eller it-problem eftersom vissa oindexerade hemsidor inte har ett tillräckligt skydd för besökaren.

Det bör anses vedertaget att det på ”Deep web” döljer sig brottslig aktivitet på samma sätt som det gör på det indexerade internet. Hur stor omfattning det sker i saknas det idag uppgifter om likt det saknas 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.

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. Detta leder eventuellt även tankarna till nätverk som syftar till att dela olagligt material. Även om så skulle vara fallet innebär det inte att alla ”Darknets” utnyttjas för sådana syften. Tor-nätverket har tydligt syftet att tillhandahålla privatpersoner skydd för sin personliga integritet och företag skydd för företagshemligheter. Detta framgår bland annat genom marknadsföringen av Tor samt genom nätverkets hemsida vilket kommer att beröras närmare senare i denna rapport.

Att Tor-nätverket figurerat i media i samband med brottsliga aktiviteter exempelvis gällande tillslaget mot hemsidan ”Silk road”[15] som var en marknadsplats för allt från droger till lönnmördare har troligtvis påverkat allmänhetens uppfattning om Tor-nätverket. Men det finns idag inga direkta bevis för att en större del av trafiken i Tor är kopplad till brottslig verksamhet än trafiken på internet generellt. Det kan därför inte endast baserat på medias rapportering och chattrådar på diskussionsforum anses vara vedertaget att Tor i huvudsak används för brottsliga verksamhet.

[15] FBI stängde ökänd drog- och vapenhandelssajt, Bie, Nanok, den 2 oktober 2013, uppdaterad 9 oktober 2013, http://www.svt.se/nyheter/utrikes/okanda-drog-och-vapenhandelssajten-silk-road-nedstangd.

1. Tekniken

1.1 Tor

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.[16]

NRL offentliggjorde i början av 2000-talet[17] koden till mjukvaran gratis som en öppen programvara. 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.[18]

Idag finns det dagligen strax över två miljoner användare av Tor, men denna siffra förändras kontinuerligt.[19]

1.1.1 Nätverket

De som vill använda Tor kan välja att antingen bara utnyttja nätverket och då vara en *klient*[20] eller tillhandahålla Tor-noder och då vara *tillhandahållare*. För att bli klient i Tor behöver

[16] Översikt av Tor, https://www.torproject.org/about/overview.
[17] Meddelande om lansering av ”onion router”, den 20 september 2002, http://archives.seul.org/or/dev/Sep-2002/msg00019.html, Meddelande om lansering av Tor, den 8 oktober 2003, https://lists.torproject.org/pipermail/tor-dev/2003-October/002185.html, LevineOn Yasha, Almost everyone involved in developing Tor was (or is) funded by the US government, Panodaily, den 16 juli 2014, http://pando.com/2014/07/16/tor-spooks/, Skärmutklipp från den officiella hemsidan för Tor, https://www.evernote.com/shard/s1/sh/23cf697d-2353-4247-815c-b4efa35d8639/3ade44b5db780f279f550f9e6ecbb2ac, Hemsida om ”onion routing”, historisk exposé, http://www.onion-router.net/History.html.
[18] Officiell lista av finansiärer av Tor, https://www.torproject.org/about/sponsors.html.en.
[19] 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.
[20] 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.

användaren ladda ner Tor-mjukvaran till sin enhet[21] 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*)[22].

Att konfigurera en enhet innebär att ändra inställningar och andra åtgärder för att en enhet eller ett program ska kunna kommunicera med andra enheter eller program. I frågan om Tor-noder innebär konfigurationen att enheten ska kunna kommunicera med Tor-mjukvaran och med Tor-noder.

Den andra rollen är tillhandahållare[23] av Tor-noder. För att skapa noder laddar tillhandahållaren precis som ovan beskrivits ner mjukvaran till sin enhet men väljer istället att konfigurera sin enhet till en Tor-nod. Genom denna konfiguration kan enheten dela med sig av bandbredd och sin ip-adress till andra Tor-klienter. På detta sätt skapas noderna i Tor.

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. Det går även att konfigurera enheter till så kallade bryggnoder, vilket kommer att beröras i avsnitt 1.1.4.

När en enhet konfigureras till Tor-nod finns det tre former av funktionspaket som tillhandahållaren kan välja mellan: 1) ingångs- och mellannod, 2) ingångs-, mellan- och utgångsnod, eller 3) bryggnod. Tillhandahållaren kan alltså inte välja att exempelvis endast tillhandahålla en mellannod.

[21] Någon form av lagringsmedia, exempelvis en vanlig hemmadator eller en hyrd server i en serverhall.
[22] Officiell hemsida för Tor, ”hidden services”, https://www.torproject.org/about/overview.html.en#hiddenservices.
[23] Även om tillhandahållare själva kan använda Tor, kommer definitionen ”tillhandahållare” i denna rapport att användas för de som tillhandahåller Tor-noder i nätverket.

1.1.2 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”).[24] DA är noder konfigurerade att samla upp information om samtliga Tor-noder som är tillgängliga samt nodernas egenskaper[25]. DA skapar och publicerar sedan *consensus* en gång i timmen genom en automatiskt förprogrammerad procedur[26]. *Consensus* är en offentlig lista över alla Tor-noder och visar även vilken typ noderna är.[27] Samtliga Tor-noder förutom bryggnoder[28] går alltså att se i *consensus*. C*onsensus* hämtas av samtliga klienter så att klienternas enheter vet vilka noder trafik kan skickas. Genom att DA tilldelar noderna sina roller kan den som driver noder inte på egenhand avgöra vilken typ av nod de för tillfället ska tillhandahålla. DA kan dock bara tilldela en Tor-nod de roller som den konfigurerats för.

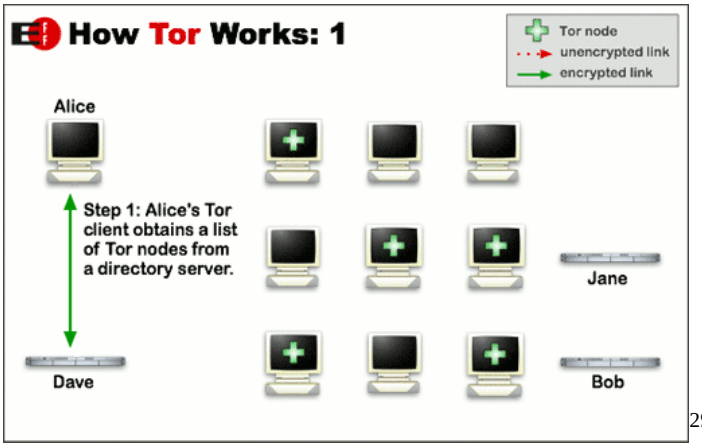
1.1.3 Hur fungerar Tor?

Beskrivningen av hur Tor fungerar kommer att göras översiktligt för att ge en grundläggande förståelse för funktionerna i Tor.

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.

[24] Det kan nämnas att det finns nio stycken DA, se https://metrics.torproject.org/about.html.
[25] En egenskap kan exempelvis vara hur mycket bandbredd noden tillhandahåller och vilken typ av funktion enheten är konfigurerad för.
[26] Proceduren innebär att samtliga DA röstar fram *consensus* genom en programmerad algoritm. Det saknas behov av fördjupning i algoritmerna och programmeringen av den för den fortsatta framställningen i denna rapport, varför detta kommer att utelämnas.
[27] Se *consensus* och dess statistik, https://consensus-health.torproject.org/.
[28] Behandling av bryggnoder kommer att göras i avsnitt 1.1.4.

Figur 1

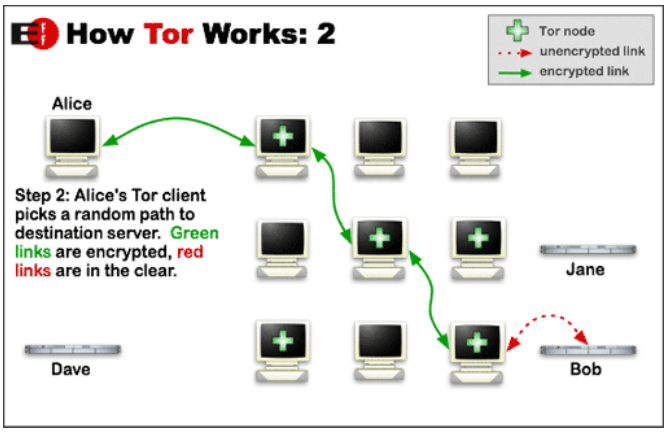


[29]

Ponera att användaren vill besöka hemsidan www.sverigesradio.se. När användaren skriver in adressen i webbläsaren skickas informationen till en ingångsnod 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 nytt uppsättning krypteringsnycklar. Samtliga krypteringsnycklar förhandlas alltså fram mellan klienten och respektive Tor-nod enskilt genom en avancerad krypteringsteknik[30] utan att klientens identitet framgår.

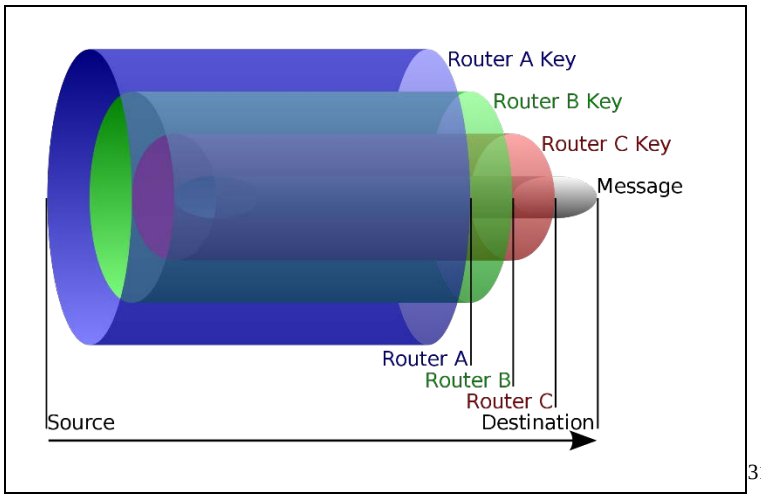
[29] Översikt av Tor, https://www.torproject.org/about/overview, Bilder använda enligt avtal: https://creativecommons.org/licenses/by/3.0/us/.
[30] Krypteringssystemet kallas Diffie–Hellman, https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange#Description.

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. Informationen som går mellan noderna är också den krypterad, vilket innebär att informationen måste avkrypteras för att kunna få information om vad det är för trafik som går genom noderna. Namnet ”onion” har Tor fått just genom att Tor skapar flera lager krypteringar, alltså fungerar krypteringen som skalen på en lök.

Figur 3



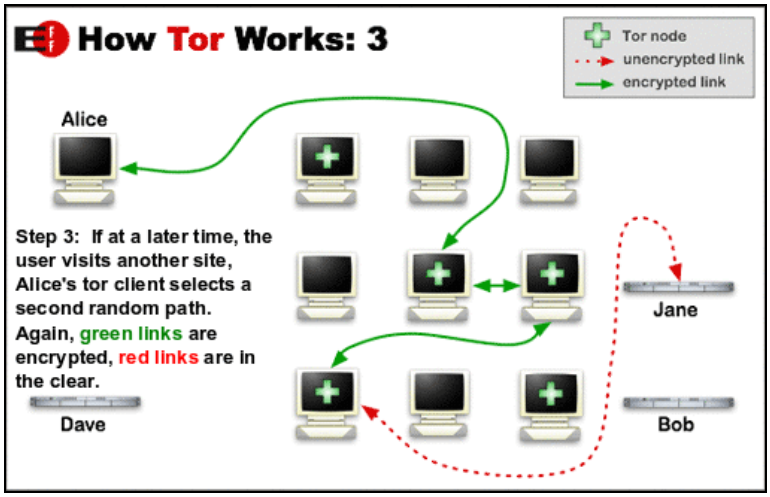
[31]

All trafik i Tor-nätverket ska hoppa tre gånger mellan noderna, aldrig fler eller färre gånger även om detta är tekniskt möjligt. När trafiken slutligen når utgångsnoden och lämnar Tor-nätverket upphör krypteringen som Tor tillför. Den som bevakar slutmålet för trafiken eller

[31] Bilden är hämtad från English Wikipedia användaren HANtwister och får publiceras i enlighet med Creative Commons Attribution-Share Alike 3.0 Unported license, https://upload.wikimedia.org/wikipedia/commons/thumb/e/e1/Onion_diagram.svg/2000px-Onion_diagram.svg.png.

utgångsnoden kan då se trafiken från utgångsnoden och var trafiken går. Denna detalj är mycket viktig för många journalister eftersom de vill att deras meddelanden ska vara skyddade hela vägen till och från sina källor. Det innebär att meddelanden som journalister skickar och tar emot, enskilt måste krypteras för att de ska vara skyddade från insyn när meddelandena lämnar Tor eftersom den kryptering som Tor tillförde då upphör.

Figur 4



När samma användare sedan vill besöka en annan hemsida används samma krets inom tio minuter från att banan senast användes av klienten. Om klienten inte använt kretsen inom tio minuter skapas en ny krets. Detta sker för att uppnå en så hög hastighet i Tor-nätverket som möjligt. Vägvalet för trafiken är som ovan beskrivits inget klienten ser eller märker av, utan enheterna ”pratar” och överför trafik till varandra och utan inblandning av användaren eller tillhandahållaren av Tor-noder. Klienten kan dock i viss mån påverka vilka Tor-noder som ska användas eller inte användas.

Det ska noteras att det alltså är utgångsnodens ip-adress som kommer 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. Detta är av stort intresse för rättsvårdande myndigheter eftersom personen som driver Tor-noden kan komma att misstänkas 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.[32]

[32] Tor FAQ, https://www.torproject.org/docs/faq.html.en#ExitPolicies.

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.

1.1.4 Tor-brygga

I vissa länder är tillgången till internet och informationen på internet begränsad och övervakad. Orsaken till begränsningarna kan vara att ISP:er blockerar eller filtrerar trafik till vissa sidor på internet. Det finns situationer där ISP:er och staten är en och samma aktör och situationer där ISP:er agerar på uppdrag från rättsväsendet i en förtryckande stat för att begränsa användares tillgång till information eller möjlighet att utbyta åsikter.

Vissa ISP:er blockerar trafik till de noder som är synliga i *consensus*. För att då kunna komma åt Tor-nätverket behöver därför vissa klienter gå via så kallade Tor-bryggor.[33] Även bryggorna är noder och driften av bryggnoder kräver likt de noder som beskrivits ovan först att mjukvara laddas ner och att enheten sedan konfigureras till bryggnod.

Efter att enheten konfigurerats till en bryggnod skickar noden information till ”bridge authority” (”BA”)[34] på samma sätt som de tidigare beskrivna noderna skickar information till DA. BA samlar på så sätt in information om samtliga bryggnoder till en lista. Dock skapar BA ingen *consensus*, utan en lista över noderna som inte är offentlig. Listan är hemlig eftersom ISP:er annars skulle kunna se vilka noder som är bryggnoder och blockera eller filtrera bort trafiken till dem. Skillnaden mellan *consensus* och listan skapad av BA är att listan inte skapas genom någon procedur samt att listan inte offentliggörs på internet såsom *consensus*.

Vid användningen av en bryggnod hoppar trafiken inledningsvis från klienten till bryggnoden. Det skapas på samma sätt som för övriga noder en krypteringstunnel mellan klienten och bryggnoden där en uppsättning krypteringsnycklar utfärdas. Därefter går trafiken vidare till en mellannod och sedan till en utgångsnod varifrån trafiken slutligen går till slutdestinationen. Samma lager av kryptering och samma krypteringsmetod som beskrivits ovan används för överföringen av trafiken.

Bryggnoder är således identiska med ingångsnoder gällande sin funktion, men skillnaden är att deras existens inte är offentlig som ingångsnodernas. I och med detta kommer driften av bryggnoder inte att beröras enskilt i rapporten utan omfattas av begreppet Tor-noder.

[33] Officiell hemsida för Tor, information om bryggnoder, https://www.torproject.org/docs/bridges.html.en.
[34] Det kan nämnas att det endast finns en BA till skillnad från DA som det finns nio stycken av. Ordlista Tor, https://metrics.torproject.org/about.html.

Del 1 Ansvar enligt lagen om elektronisk kommunikation

Inledningsvis ska i denna rapport redogöras för om skyldigheter enligt lagen om elektronisk kommunikation (”LEK”)[35] kan uppkomma för tillhandahållare av Tor-noder.

2. Bakgrund till LEK

Europeiska kommissionen (”kommissionen”) presenterade år 2000 ett förslag till ny lagstiftning på området för elektronisk kommunikation.[36] Enligt kommissionen krävdes en modern och samlad lagstiftning som stod mer i överensstämmelse med den tekniska och marknadsmässiga utvecklingen på området. Den marknadsmässiga utveckling som åsyftades var den mer konkurrensutsatta marknad som hade skapats, där fler aktörer tillhandahöll tjänster och nät för elektronisk kommunikation. Beträffande den tekniska utvecklingen låg fokus på det tekniska närmande som skett mellan telefoni, datakommunikation och media.[37] Ett nytt regelverk antogs av Europaparlamentet och rådet år 2002. Regelverket omfattar fem direktiv och ett beslut.[38]

I Sverige hade avregleringen av flera delar av den statliga monopolmarknaden vid samma tidpunkt inletts. Marknaden för telekommunikation var en av de marknader som staten hade valt att konkurrensutsätta i enlighet med den internationella trend som rådde vid tiden. Målet var och är än idag att lämna de ekonomiska besluten på marknaden helt till de enskilda aktörerna. Tanken med avregleringen var att statens inblandning på marknaden skulle begränsas till att endast avhjälpa de problem som skulle kunna stå i vägen för att uppnå en fri och öppen marknad.[39]

[35] Lag och elektronisk kommunikation (SFS 2003:389).
[36] Kommissionens förslag till direktiv om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster, KOM(2000) 393, EGT C 365 E, 19.12.2000, s. 198.
[37] Proposition 2002/03:110, *Lag om elektronisk kommunikation, m.m*, s. 64.
[38] Bestående av ett ramdirektiv Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster, och fyra särdirektiv, Europaparlamentets och rådets direktiv 2002/20/EG av den 7 mars 2002 om auktorisation för elektroniska kommunikationsnät och kommunikationstjänster, Europaparlamentets och rådets direktiv 2002/19/EG av den 7 mars 2002 om tillträde till och samtrafik mellan elektroniska kommunikationsnät och tillhörande faciliteter, Europaparlamentets och rådets direktiv 2002/22/EG av den 7 mars 2002 om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster, Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation och Europaparlamentets och rådets beslut nr 676/2002/EG av den 7 mars 2002 om ett regelverk för radiospektrumpolitiken i Europeiska gemenskapen (radiospektrumbeslut).
[39] Prop. 2002/03:110, s. 58.

LEK:s huvudsyfte är alltså att öka konkurrensen på marknaden för elektronisk kommunikation genom att sänka gränserna för inträde på marknaden.[40]

Det är viktigt att påpeka att tillämpningsområdet för LEK inte omfattar innehållet i den trafik som överförs via kommunikationsnät eller kommunikationstjänster.[41] LEK reglerar endast själva näten och de tjänster som möjliggör överföring av innehåll. Reglering gällande innehållet i elektroniska kommunikationstjänster finns istället i e-handelslagen (”EHL”)[42], som i stora delar är konsumenträttslig.[43] Exempel på tjänster som omfattas av EHL är, förutom e-handel: informationstjänster, finansiella tjänster, fastighetsmäklartjänster, webbhotell och söktjänster, så länge de tillhandahålls via internet.[44]

När datalagringsdirektivet[45] sedan publicerades, valde Sverige att implementera bestämmelserna i LEK.[46] Lagstiftaren valde att göra skyldigheten att lagra data avhängigt anmälningsplikten i LEK, med hänvisning till datalagringsdirektivet.[47] Förutsättningen för att sammanlänka anmälningsplikten med datalagringsskyldigheten var att lagstiftaren vid skapandet av LEK valde att införa anmälningsplikt för viss verksamhet, vilket inte var ett tvång för medlemsstaterna.[48]

Datalagringsdirektivet ogiltigförklarades av EU-domstolen år 2014.[49] Regeringen i Sverige utredde efter att domen kom hur Sverige skulle agera och kom fram till att Sverige fortsatt ska tillämpa de regler som baserar sig på datalagringsdirektivet. Anledningen till detta är enligt utredaren att den information som lagras enligt svensk rätt anses tillräckligt skyddade och tillgången till uppgifterna tillräckligt strikt reglerade för att lagringen ska anses proportionerlig, vilket inte ansågs vara fallet i målet hos EU-domstolen.[50] Därför har

[40] Prop. 2002/03:110, s. 66.
[41] LEK 1:4.
[42] Lag om elektronisk handel och andra informationssamhällets tjänster (SFS 2002:562).
[43] Proposition 2001/02:150, Lag om elektronisk handel och andra informationssamhällets tjänster, m.m., s. 22.
[44] Prop. 2001/02:150, s. 19.
[45] 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.
[46] Lag (SFS 2012:127) om ändring i lagen (SFS 2003:389) om elektronisk kommunikation.
[47] LEK 6:16a, LEK 2:1 samt datalagringsdirektivet artikel 1 och 3.
[48] Proposition 2010/11:46, *Lagring av trafikuppgifter för brottsbekämpande ändamål - genomförande av direktiv 2006/24/EG*, s. 43.
[49] Europeiska unionens domstol den 8 april 2014 genom de förenade målen C-293/12 och C-594/12 Digital Rights Ireland och Seitlinger m.fl. mot Minister for Communications, Marine and Na¬tural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irland, The Attorney General, Regeringen (”Digital Rights Ireland och Seitlinger m.fl. mot Minister for Communications m.fl.”).
[50] Ds 2014:23, *Datalagring EU-rätten och svensk rätt*, s. 99.

regleringen gällande datalagring fortfarande relevans för redogörelsen om anmälningsplikt eftersom det är en direkt konsekvens av anmälningsplikten.

2.1 Anmälningsplikten

Auktorisationsdirektivet[51], tar sikte på att öka friheten för tillhandahållande av *elektroniska kommunikationsnät* och *tjänster* genom att begränsa de administrativa hindren för inträde på marknaden för dessa aktörer. För att åstadkomma detta infördes förbud mot krav på *särskild auktorisation* för verksamhet inom området för elektronisk kommunikation, dock tilläts medlemsstaterna att införa *anmälningsplikt* för vissa aktörer.[52]

Lagstiftaren i Sverige valde att införa anmälningsplikt för aktörer som tillhandahåller *allmänna kommunikationsnät mot ersättning* samt aktörer som tillhandahåller *allmänt tillgängliga elektroniska kommunikationstjänster*.[53] De aktörer som är anmälningspliktiga har ytterligare skyldigheter att bland annat tillhandahålla särskilda tjänster för totalförsvarets behov och samhällets alarmerings- och räddningstjänst samt att beakta funktionsvariationer bland användarna av aktörens verksamhet.[54]

Argumenten för införande av anmälningsplikt var dels behovet av kännedom om aktörerna på den svenska marknaden och dels behovet av att utöva nödvändig tillsyn över dessa aktörer, något lagstiftaren menade endast kunde uppnås genom införande av anmälningsplikt.[55] I och med att anmälningsplikten efter implementeringen av datalagringsdirektivet blev kopplad till kravet på datalagring fick kravet på anmälningsplikt större verkningar för de anmälningspliktiga aktörerna. De anmälningspliktiga aktörerna blev som huvudregel[56] nu förpliktade att samla in och spara information om sina användare.

Det främsta syftet med LEK är som ovan nämnts att öka konkurrensen på marknaden för elektronisk kommunikation. Denna grundpremiss ges stort utrymme vid bedömningen av vad som är anmälningspliktig verksamhet och inte. Anledningen till denna utgångspunkt är att anmälningsplikt skapar hinder för marknadstillträde för nya aktörer. Mot bakgrund av detta finns det skäl att låta redogörelsen och tolkningen av lagtexten och förarbetena strikt hålla sig till lagstiftningens uttryckliga syfte. Även Post- och Telestyrelsen (”PTS”) uttrycker att det är

[51] Europaparlamentets och rådets direktiv 2002/20/EG av den 7 mars 2002 om auktorisation för elektroniska kommunikationsnät och kommunikationstjänster.
[52] Prop. 2002/03:110, s. 66.
[53] LEK 2:1.
[54] Prop. 2002/03:110, s. 85.
[55] SOU 2002:60, *Lag om elektronisk kommunikation*, s. 20 samt prop. 2002/03:110, s. 121.
[56] Undantag från datalagring kan medges enligt LEK 6:16b.

syftet med lagstiftningen som ska vägleda vid bedömningar av vilka nät och tjänster som ska omfattas av LEK.[57]

[57] Vilka tjänster och nät omfattas av LEK? En vägledning, PTS-ER-2009:12, 2009-03-11, http://www.pts.se/upload/Rapporter/Internet/2009/ekomtjanster-2009-12.pdf, s. 14.

3. Allmänna kommunikationsnät

LEK 1:7 *allmänt kommunikationsnät*:

> ”[…]elektroniskt kommunikationsnät som helt eller huvudsakligen används för att tillhandahålla allmänt tillgängliga elektroniska kommunikationstjänster och som stödjer informationsöverföring mellan nätanslutningspunkter,”.

Definitionen är beroende av definitionen av *elektroniskt kommunikationsnät* vilket framgår av samma bestämmelse:

> ”[…] system för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt passiva nätdelar och andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier oberoende av vilken typ av information som överförs,”.

Dessa definitioner i LEK är identiska med de i ramdirektivet[58].[59] Definitionen av elektroniskt kommunikationsnät tar bland annat sikte på både fysiska och logiska nät. Ett logiskt nät innebär att enheter är sammankopplade med varandra och bildar ett virtuellt nät där särskilda kommunikationsprotokoll används för kommunikationen, ett exempel på logiskt nät är internet.[60]

Eftersom Tor-noder genom konfigurationen är sammankopplade virtuellt torde Tor närmast kunna liknas vid ett logiskt nät enligt definitionen. Tor-noderna medger även överföring av signaler genom att ta emot signaler från klienter och vidarebefordra dem till andra Tor-noder eller till en slutdestination genom att dela med sig av sin bandbredd, med andra ord överföringskapacitet, vilket ytterligare indikerar att Tor skulle kunna utgöra ett logiskt nät.

Under förutsättning att Tor utgör ett logiskt nät uppkommer frågan om vem som ska anses vara tillhandahållare av nätverket. Ska samtliga tillhandahållare av Tor-noder anses vara tillhandahållare eller innebär konstruktionen av nätverket att endast vissa tillhandahållare eller rent av någon annan exempelvis Tor-project är den som tillhandahåller nätverket. Denna fråga

[58] Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster.
[59] Prop. 2002/03:110, s. 116.
[60] SOU 2001:28, *Yttrandefrihetsgrundlagen och Internet. Utvidgat grundlagsskydd och andra frågor om tryck- och yttrandefrihet*, s. 136 samt SOU 2002:60, s. 131.

kommer här inte närmare att beröras utan utgångspunkten för den fortsatta redogörelsen är att samtliga tillhandahållare bör anses vara tillhandahållare av det logiska nätet.

3.1. Vanligen mot ersättning

För att omfattas av anmälningsplikt krävs dock även att nätet vanligen tillhandahålls mot ersättning.[61] I förarbetena anges att elektroniska kommunikationsnät som tillhandahålls för kommersiellt bruk omfattas av anmälningsplikten, utan att närmare gå in på vad kommersiellt bruk innebär.[62] Ledning behöver därför tas ur förarbetsuttalandena gällande kravet tillhandahållande av elektroniska kommunikationstjänster som också de omfattas av kravet på ”vanligen mot ersättning”.[63]

Kravet innebär inte att det i samtliga fall krävs att någon ersättning utgår till den som tillhandahåller tjänsten. I förarbetena ges reklamfinansiering som exempel på när tjänsten ska anses uppfylla definitionens krav.[64] I fallet med reklamfinansiering är det en tredje part, den som betalar för reklamen, som står för ersättningen till tillhandahållaren, inte användaren själv. Användaren blir dock exponerad för reklamen som en tredje part betalar för och det kan antas vara lagstiftarens mening att tjänsten på så sätt ska anses tillhandahållas mot ersättning. Uttryckt på ett annat sätt, användarens motprestation är att bli ”utsatt” för reklam i utbyte mot att få använda tjänsten.

I fallet med Tor-noder är frågan något mer komplex. Som förklarats i avsnitt 1.1 är mjukvaran till Tor gratis. Den som väljer att tillhandahålla en Tor-nod behöver inte betala något för mjukvaran, dock behöver tillhandahållaren betala en ISP för tillgång till internet för att få tillgång till mjukvaran samt för att kunna tillhandahålla Tor-noder. Detta innebär inledningsvis att Tor-project inte kan anses tillhandahålla mjukvaran för kommersiellt bruk i detta avseende.

Användarna som i sin tur också laddar ner mjukvaran och konfigurerar sin enhet behöver inte heller de betala Tor-project eller exponeras för någon reklam när detta sker. Men även användarna behöver tillgång till internet och därför betala en ISP för att kunna få tillgång till Tor.

Användarna behöver inte heller när de utnyttjar Tor betala något för tjänsten mer än till sin egen ISP. De blir inte heller på grund av användningen av Tor exponerade för reklam under

[61] LEK 2:1.
[62] Prop. 2002/03:110, s. 362.
[63] LEK 2:1.
[64] Prop. 2002/03:110, s. 358.

tiden de använder Tor. Användarna betalar alltså inte till tillhandahållarna av Tor-noder för att få utnyttja deras bandbredd och ip-adress.

Eftersom Tor finansieras av statliga myndigheter, organisationer samt privatpersoner,[65] blir frågan dock om det kan ses som att en tredje part har finansierat Tor på samma sätt som vid reklamfinansiering vilket skulle leda till att tillhandahållande av Tor-noder sker för kommersiellt bruk.

Som ovan beskrivits torde synen på vad som ska anses vara *mot ersättning* innebära att vardera part presterar något. Vid reklamfinansiering bör det som ovan sagts ses som att den som blir exponerad för reklamen vid användandet av nätverket eller tjänsten presterar i form av att se reklamen.

Motprestationerna behöver alltså ha någon form av direkt samband med parterna i fråga. I fallet med finansieringen av mjukvaran från tredje part finns det ingen motprestation från användaren, eftersom användaren inte exponeras för någon form av information eller reklam om exempelvis vem som har finansierat utvecklingen av mjukvaran.

Inte heller rör det sig om någon reciprocitet mellan den som tillhandahåller Tor-noder och användaren eftersom det endast är tillhandahållaren som presterar genom att tillgängliggöra bandbredd, överföring av signaler samt kryptering av trafiken i nätverket och användaren endast utnyttjar detta.

Tillhandahållande av Tor-noder bör därför kunna anses vara av helt ideell karaktär och skulle därmed också troligvis undantas från LEK.[66] Det faktum att användarna betalar för sin internetuppkoppling kan inte anses vara en motprestation eftersom det inte är ett utbyte av prestationer mellan de som tillhandahåller Tor-noder och användarna.

Mot bakgrund av detta kommer någon fortsatt redogörelse angående bland annat fysiska nät inte att göras här då frågan om kommersiellt bruk är avgörande för anmälningspliktens omfattning.

[65] Officiell lista av finansiärer av Tor, https://www.torproject.org/about/sponsors.html.en.
[66] Prop. 2002/03:110, s. 358.

4. Allmänt tillgängliga elektroniska kommunikationstjänster

I LEK 1:7 definieras *elektronisk kommunikationstjänst* som:

> ”[…] tjänst som vanligen tillhandahålls mot ersättning och som helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät,”

En *elektronisk kommunikationstjänst* är i sig inte anmälningspliktig eftersom det av LEK 2:1 framgår att den *elektroniska kommunikationstjänsten* också behöver vara *allmän* för att anmälningsplikt ska föreligga.

Definitionen elektronisk kommunikationstjänst är identisk med den i ramdirektivet[67]. Det som är av intresse är att det i ramdirektivet och i LEK[68] tydliggörs att *innehållstjänster* undantas från definitionens omfång och genom det också från lagstiftningens tillämpningsområde.

4.1. Innehållstjänst

Det framgår inte av ramdirektivet vad som menas med innehållstjänster. I förarbetena till LEK görs bedömningen att ”innehåll” bör anses vara intellektuellt innehåll och budskap som går att mottas genom röster, bilder och liknande.[69] I förarbetena ges även exempel på innehållstjänster i form av hemsidor för elektronisk handel och sidor där musik och spel tillhandahålls.[70]

Som beskrivits är Tor en krypteringstjänst som möjliggör att signaler överförs genom att badbredd från enheter utnyttjas. Tillhandahållare av Tor-noder tillhandahåller därför inte något intellektuellt innehåll till användarna, utan endast tillgång till en ip-adress, bandbredd och kryptering. Därför kan Tor inte anses vara en innehållstjänst och kan därmed inte grundat på det undantas från LEK.

4.2. Tjänst som helt eller huvudsakligen utgörs av överföring av signaler i det elektroniska kommunikationsnätet

Frågan är om tillhandahållande av Tor utgör en tjänst som *helt eller huvudsakligen utgörs av överföring av signaler i det elektroniska kommunikationsnätet*.[71]

Signaler innebär analog eller digital data som kan överföras via elektromagnetiska vågor och som kan innehålla data i form av text, ljud, bild och kombinationer av dessa.[72] I

[67] Europaparlamentets och rådets direktiv 2002/21/EG, artikel 2.c.
[68] LEK 1:4 st. 2.
[69] SOU 2002:60, s. 155.
[70] Prop. 2002/03:110, s. 358-359.
[71] Prop. 2002/03:11, s. 116.

ramdirektivet[73] ges teletjänster och överföringstjänster i nät som används för rundradio som exempel på tjänster som inryms i definitionen. I förarbeten till annan lagstiftning som hänvisar till LEK ges exempel som fast telefoni, mobiltelefoni, internet och e-post.[74]

Eftersom det i förarbetena inte ges någon närmare förklaring till vad som menas med överföring av signaler behöver en egen slutsats dras om vad det kan betyda. Baserat på de exempel som ges i både förarbetena och i ramdirektivet, är en möjlig slutsats att det är själva funktionen att överföra signaler som menas i lagstiftningen.

Huvudsyftet med Tor är som tidigare nämnts att kryptera signaler samt att möjliggöra överföring av trafik genom tillhandahållarens bandbredd och utnyttjande av ip-adress. Det kan konstateras att det överförs signaler genom Tor-noderna. Det är dock oklart om det kan antas att tillhandahållare av Tor-noder utför själva överföringstjänsten. En möjlig slutsats skulle vara att det är respektive tillhandahållares ISP som tillhandahåller överföringstjänsten och att tillhandahållare av Tor-noder endast tillhandahåller en form av applikation som möjliggör kryptering och anonymisering. Det faktum att noderna är en förutsättning för att trafik ska överföras i nätverket bör dock kunna leda till slutsatsen att tillhandahållare även tillhandahåller en överföringstjänst.

Var gränsen går för vad som är huvudsaklig överföring av signaler är inte klarlagd i någon procentsats eller liknande utan får avgöras genom en samlad bedömning av tjänsten. Gällande Tor skulle slutsatsen inte osannolikt kunna vara att tillhandahållande av bandbredd utgör en så pass stor del av funktionen i Tor att Tor får anses utgöra en sådan överföringstjänst som kan omfattas av definitionen i LEK.

4.3. Vanligen mot ersättning

Utöver utformningen av tjänsten krävs det enligt definitionen samt bestämmelsen om anmälningsplikt att tjänsten vanligen utförs mot ersättning.[75]

Gällande begreppet vanligen mot ersättning bör samma bedömning göras som redogjorts för i avsnitt 3.1, varför slutsatsen alltså torde vara att tjänsten inte tillhandahålls mot ersättning i legens mening då det inte sker någon motprestation från användarna.

---

[72] Prop. 2002/03:11, s. 111 och SOU 2002:60, s. 109.
[73] Europaparlamentets och rådets direktiv 2002/21/EG, artikel 2.c.
[74] Proposition 2005/06:195 Elektroniska kommunikationstjänster m.m. inom psykiatrisk tvångsvård, s. 19.
[75] LEK 1:7 samt LEK 2:1

4.4. Summering

Det råder fortfarande oklarheter kring hur tillhandahållande av Tor-noder ska bedömmas utifrån reglerna i LEK.

Tor-nätverket bör kunna utgöra ett elektroniskt kommunikationsnät enligt lagens definition eftersom det troligtvis utgör ett logiskt nätverk. Tillhandahållande av Tor-noder bör även kunna anses utgöra en elektronisk kommunikationstjänst eftersom noderna möjliggör överföring av signaler i Tor-nätverket.

Däremot bör tillhandahållande av Tor-noder kunna undantas anmälningsplikt eftersom Tor inte bör kunna anses tillhandahållas mot ersättning enligt lagens krav då det inte sker någon motprestation från användarna.

Det ska därför konstateras att tillhandahållare av Tor-noder inte bör vara anmälningspliktiga för att tillhandahålla Tor-noder. Vilket i sin tur innebär att det inte finns några krav på att lagra information om användarna av Tor-noderna.

Del 2 Straffrättsligt ansvar

5. Inledning

Tillhandahållande av Tor-noder innebär inte bara en möjlighet för personer att skydda sin identitet för skäl som är skyddade av rättsordningen. Anonymiteten som internet i sig medför har redan skapat problem för rättsvårdande myndigheter gällande identifieringen av personer som begår brott. Den anonymitet som Tor medför innebär därför ytterligare svårigheter för rättsvårdande myndigheter att kunna identifiera och beivra brott. Frågan som uppstår i och med detta är om de som tillhandahåller Tor-noder på något sätt kan hållas straffrättsligt ansvariga för tillhandahållandet i sig eller för medverkan till ett brott som en användare begår.

I denna del ska ges en bakgrund till hur straffrätten ser ut idag och hur straffrättsliga bedömningar görs av Sveriges domstolar, för att ge en bakgrund och förståelse för hur en prövning av tillhandahållande av Tor-noder skulle kunna se ut i en domstolsprocess.

Brottsbalken[76] (”BrB”) är den huvudsakliga straffrättsliga lagstiftningen i Sverige och innehåller en uppräkning av olika typer av brott såsom rån[77], stöld[78] och misshandel[79]. BrB innehåller även regler om när en otillåten handling är rättfärdigad, alltså när en handling på grund av omständigheterna är tillåten men som i vanliga fall skulle varit otillåten eller när en brottslig handling är ursäktad[80], alltså när ett brott faktiskt har begåtts men omständigheterna gör att personen i fråga inte ska dömas för brottet. BrB innehåller också regler om vilka straff som finns och kan utdömas[81] för olika brott.

Utöver BrB finns den så kallade specialstraffrätten. Specialstraffrätten omfattar de lagar som reglerar brott inom särskilda områden, exempelvis narkotikabrott[82], trafikbrott[83] och miljöbrott[84]. Inom specialstraffrätten finns även särskilda lagar om terrorism som direkt hänvisar till brott i BrB eller innehåller en uppräkning av brottsbeskrivningar som återfinns i

[76] Brottsbalk (SFS 1962:700).
[77] BrB 8:5.
[78] BrB 8:1.
[79] BrB 3:5.
[80] BrB 24 kap.
[81] BrB 29 kap.
[82] Narkotikastrafflag (SFS1968:64).
[83] Lag om straff för vissa trafikbrott (SFS 1951:649).
[84] Miljöbalk (SFS 1998:808), 29:1.

BrB.[85] När det refereras till straffrätten omfattas alltså både BrB och all specialstraffrätt i begreppet.

Flertalet brott kan idag begås via internet bland annat barnpornografibrott[86], olaga hot[87] och bedrägeri[88].[89] 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.[90] Denna slutsats drog Svea hovrätt baserat på en tidigare dom från Högsta domstolen (”HD”)[91] där HD fastställde att det inte krävs fysisk närvaro för att kunna bli dömd för sexuellt övergrepp mot barn[92].[93] Frågan om bland annat sexuellt övergrepp mot barn[94] via internet avgjordes återigen av Svea Hovrätt i mars 2016.[95] Frågan om brotten kunde utföras över internet var i denna dom inte någon reell fråga utan det verkar nu anses vara en självklarhet 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.[96] Den åtalade personen dömdes dock för flera andra brott bland annat sexuellt övergrepp mot barn, utnyttjande av barn för sexuell posering[97], sexuellt ofredande[98] och barnpornografibrott[99].

Brott som begås på internet kallas vanligen för ”IT-relaterade brott” medan begreppet ”IT-brott” normalt används för att beteckna dataintrång[100] eller datorbedrägeri[101].[102]

Internet möjliggör att brott kan begås på flera platser i världen samtidigt utan att gärningspersonen behöver närvara fysiskt på dessa platser vilket bland annat leder till gränsdragningsproblem gällande vilka lagar och regler som ska tillämpas, alltså vilken

[85] Lag om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet (SFS 2010:299) samt Lag om straff för terroristbrott (SFS 2003:148).
[86] BrB 16:10 a.
[87] BrB 4:5.
[88] BrB 9:1.
[89] *It-relaterade brott - polisens arbete*, https://polisen.se/Om-polisen/Olika-typer-av-brott/IT-brott/.
[90] Mål nr B 6051-15, Svea hovrätt, 2015-09-09, s. 8.
[91] NJA 2015 s. 501.
[92] BrB 6:6.
[93] NJA 2015 s. 501, s. 5-7.
[94] BrB 6:6.
[95] Mål nr B 5801-15, Svea hovrätt, 2016-03-01.
[96] Mål nr B 1687-14, Attunda tingsrätt, 2016-06-23, s. 52.
[97] BrB 6:8.
[98] BrB 6:10.
[99] BrB 16:10a.
[100] BrB 4:9 c.
[101] BrB 9:1 st. 2.
[102] *It-relaterade brott - polisens arbete*, https://polisen.se/Om-polisen/Olika-typer-av-brott/IT-brott/.

jurisdiktion som gäller för händelserna. Den fortsatta redogörelsen i denna rapport kommer dock 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.

6. Grunderna för en straffrättslig bedömning

6.1. Legalitetsprincipen

En grundbult i ett demokratiskt samhälle är att medborgarna inte godtyckligt ska kunna straffas för sina handlingar utan det ska finnas tydliga regler om vilka handlingar som inte är tillåtna och vilka straff som kan komma att åläggas den som handlar i strid med reglerna.

Legalitetsprincipen kallas den princip som befäster detta och innebär den yttersta ramen för straffrättsligt ansvar vilken är att straff inte ska kunna utdömas om det saknas direkt stöd i lag eller annan författning för detta.[103] Principen kan sägas vara lagfäst i grundlag genom Regeringsformen[104] och i Europakonventionen[105].

Ett viktigt syfte med legalitetsprincipen är att en person ska kunna förutse att en handling som vidtas är brottslig och att personen kan komma att bestraffas för detta. Tanken är alltså att personen vet vad som är rätt och fel men ändå medvetet väljer att göra ”fel”. Legalitetsprincipen hänger även nära samman med *konformitetsprincipen* som innebär att en person måste ha haft möjlighet att rätta sig efter lagen men inte gjort detta för att kunna påförs ett straff.[106]

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.[107]

Legalitetsprincipen kan alltså sägas vara grunden för all tolkning och bedömning i straffrätten och kommer även i denna rapport ligga till grund för den fortsatta redogörelsen och bedömningarna.

[103] SOU 1988:7, *Frihet från ansvar-Om legalitetsprincipen och allmänna grunder för ansvarsfrihet*, s. 43.
[104] Kungörelse om beslutad ny regeringsform (SFS 1974:152), 2:10 st. 1.
[105] Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, artikel 7.
[106] Asp, Petter och Ulväng, Magnus, Kriminalrättens grunder, 2., omarb. uppl., Iustus, Uppsala, 2013, s. 46.
[107] Asp, Ulväng och Jareborg, s. 46.

6.1.1. Bevisning och beviskrav

I Sverige tillämpas fri bevisföring och fri bevisprövning enligt rättegångsbalken (”RB”).[108] Det innebär att all form av bevisning får läggas fram vid en rättegång, oavsett hur parterna har fått tag i bevisningen. Detta är en skillnad mot det vi kan se i till exempel det amerikanska rättssystemet där bevisning kan förklaras ogiltig ”inadmissible” och lämnas utan avseende. Det finns dock regler för hur bevisning ska läggas fram och liknande, men detta är processuella frågor som inte kommer att beröras i denna rapport.

Det finns dock krav på graden av hur säkert det är att en person har begått ett brott, detta kallas för *beviskrav*. Inom straffrätten är beviskravet ”ställt utom rimligt tvivel”[109] vilket är ett högt ställt krav som alltså innebär att det inte ska finns några rimliga tvivel om att ett brott har blivit begånget av den åtalade personen.

Processer i brottmål ska även genomsyras *oskyldighetspresumtion* alltså att en person är ”oskyldig tills motsatsen bevisas” och uttrycket ”hellre fria än fälla” finns lagfäst i omröstningsreglerna i RB och bör också tas i beaktande vid bedömningar inom straffrätt. Det är därför åklagaren i brottmål ska bevisa att en person är skyldig och inte den åtalade som ska visa att denne är oskyldig till brott.[110]

6.2. Straffrättslig bedömning steg för steg

För att kunna konstatera att ett brott har begåtts och att någon ska hållas ansvarig för det krävs att en prövning görs. Förenklat görs prövningen i fyra steg. Detta kan te sig något stelbent, men för att uppnå en rättssäker prövning av varje enskilt fall krävs att en viss strikthet iakttas. Inom varje steg ryms flera olika parametrar utöver lagtext och förarbeten hämtade från rättspraxis och från forskningen. Redogörelsen nedan är en förenkling av hur prövningen går till, men syftar till att ge läsaren en grundläggande förståelse för hur prövningen görs och vilka vägar en prövning kan ta.

6.2.1. Brottsbeskrivningsenlighet

Det första steget i den straffrättsliga bedömningen är att se om det som inträffat matchar någon beskrivning av brotten i BrB eller specialstraffrätten, om det matchar föreligger så

[108] Rättegångsbalk (SFS 1942:740).
[109] Asp, Ulväng och Jareborg, s. 267.
[110] Ekelöf, Per Olof, Edelstam, Henrik & Heuman, Lars, Rättegång. H. 4, 7., omarb. och rev. uppl., Norstedt, Stockholm, 2009, s. 14.

kallad *brottsbeskrivningsenlighet*.[111] Detta görs genom att ”bocka av” krav i lagtexten kallat *rekvisit*.

Ponera att A har slagit B i ansiktet detta skulle kunna vara misshandel enligt BrB 3:5:

> ”Den som tillfogar en annan person kroppsskada, sjukdom eller smärta eller försätter honom eller henne i vanmakt eller något annat sådant tillstånd, döms för misshandel”

Rekvisiten i paragrafen är alltså att 1) någon (en person) ska 2) tillfoga, 3) en annan person, 4) kroppsskada, sjukdom eller smärta eller försätta denna i vanmakt eller något annat sådant tillstånd. Om 1-3 har inträffat i verkligheten kan vi förenklat konstatera att det föreligger brottsbeskrivningsenlighet.

6.2.1.1. Kausalitet

Orsakssamband eller *kausalitet*, som det kallas i juridiken, mellan handlingen och följen krävs för att brottsbeskrivningsenlighet ska kunna föreligga.[112] Alla handlingar som på något sätt kan leda fram till ett visst resultat anses inte omfattas av sådan kausalitet som kan leda till straffrättsligt ansvar. Även om kausalitet i straffrätten är ett brett definierat begrepp finns det situationer när handlingar som någon vidtagit ligger för ”lång” ifrån det åstadkomna resultatet för att det ska anses vara relevant. Ponera exempelvis att någon smittar en annan person med HPV-virus och efter flera år får denna livmoderhalscancer till följd av detta och dör senare, eller att någon hotar en annan person så att denna lämnar en tillställning och på vägen därifrån blir påkörd av ett fordon och dör. I dessa situationer anses resultatet av personens handlande inte ligga i tillräckligt nära samband för att de ska kunna bli frågan om dråp eller mord exempelvis. Resultatet behöver således ligga tillräckligt nära gärningspersonens handling för att gärningspersonen ska ha viss kontroll över händelseförloppet.

Om brottsbeskrivningsenlighet har konstaterats genom att handlingen har matchat någon bestämmelse och det finns kausalitet mellan personens handlande och resultatet ska det kontrolleras att inga nationella begränsningar föreligger för att ett brott ska vara begånget. Hur detta görs kommer inte att beskrivas här eftersom förutsättningarna i denna rapport är att det är svensk jurisdiktion som gäller.

[111] Asp, Ulväng och Jareborg, s. 60 ff.
[112] Asp, Ulväng och Jareborg, s. 79.

6.2.2. Rättfärdigande omständigheter

Nästa steg i prövningen är att kontrollera om det saknas så kallade *rättfärdigande omständigheter* såsom nödvärn[113]; när en handling vidtagits för att skydda sig själv från exempelvis våld eller hot om våld, en annan rättfärdigande omständighet är nöd[114]; då någon handlat för att undanröja hot mot liv och hälsa.[115]

Samtycke[116] är också en rättfärdigande omständighet. För att ett samtycke ska anses utgöra en rättfärdigande omständighet krävs att: 1) samtycket föreligger under hela handlingen, 2) den som samtycker har rätt att samtycka till gärningen, 3) den som samtycker förstår innebörden av samtycket, 4) samtycket är lämnat frivilligt, 5) samtycket är allvarligt menat och 6) att gärningen som personen samtycker till inte är *oförsvarlig*. Att gärningen som personen samtycker till inte får vara oförsvarlig innebär exempelvis att en person aldrig kan samtycka till att bli mördad.[117]

Ytterligare en rättfärdigande omständighet är något som kallas för *social adekvans*. Social adekvans är en oskriven regel och tillämpas oftast i hälso- och sjukvård samt i sportsammanhang.[118] Regeln innebär att vissa handlingar som förvisso är brottsbeskrivningsenliga är rättfärdigande i förhållande till sociala normer och att det skulle vara orimligt att straffbelägga gärningarna i vissa situationer. Att genomföra en akut operation på en person är de facto misshandel men anses ändå vara ett tillåtet risktagande och är rättfärdigat enligt social adekvans.[119] Social adekvans kan även tillämpas i fall där det finns ett värde som är så viktigt, exempelvis yttrandefrihet, att någon som vanligtvis skulle vara en otillåten handling tillåts till förmån för att säkra det ”högre värdet”. Detta sätt att se på social adekvans kommer att diskuteras vidare i avsnitt 8.4.

Om det kan konstateras att det föreligger brottsbeskrivningsenlighet och att det saknas rättfärdigande omständigheter har det begåtts en *otillåten gärning*. Detta betyder ännu inte att det kan konstateras att en brottslig gärning har begåtts, men redan en otillåten gärning kan leda till *medverkansansvar* vilket kommer att förklaras närmare nedan.

[113] BrB 24:1.
[114] BrB 24:4.
[115] Asp, Ulväng och Jareborg, s. 63 f.
[116] BrB 24:7.
[117] Asp, Ulväng och Jareborg, s. 232 f.
[118] Asp, Ulväng och Jareborg, s. 255.
[119] Asp, Ulväng och Jareborg, s. 258.

6.2.3. Det allmänna skuldkravet

I det tredje steget ska det bedömas om det *allmänna skuldkravet* är uppfyllt, vilket innebär att gärningspersonen måste ha agerat med *uppsåt* eller i föreskrivna fall *oaktsamt*.

Huvudregel i svensk straffrätt enligt BrB 1:2 st.1 är att det krävs uppsåt för att personligt ansvar ska kunna utkrävas. För att oaktsamhet ska kunna leda till ansvar krävs att det framgår uttryckligen av lagregeln att det räcker med oaktsamhet. En domstol kan alltså inte bestämma att ett brott begåtts genom oaktsamhet på eget bevåg vilket följer av legalitetsprincipen som beskrivits i avsnitt 6.1.

Eftersom ”tankar inte är straffbara” i Sverige krävs det mer än bara vilja, beslutsamhet eller en åsikt för att uppsåt ska föreligga. Det krävs att tanken eller viljan ska ha kommit till fysiskt uttryck på något sätt genom handlande.

Uppsåtsbegreppet anses bestå av två delar. Den ena delen är gärningspersonens inställning eller attityd till sin gärning och följderna av denna gärning (vilja/*voluntativt element*), den andra delen är gärningspersonens tro eller kunskapsbaserade föreställning om fakta rörande omständigheterna (*kognitivt element*).[120] Enkelt uttryckt vad gärningspersonen ville skulle inträffa och vad gärningspersonen förstod om omständigheterna vid tidpunkten för händelsen. För att avgöra uppsåt hos gärningspersonen krävs att en bedömning av båda dessa delar görs och samspelet dem emellan klarläggs.

Det är här viktigt att förklara några termer mer i detalj. Begreppet *handling* som används i denna rapport innebär ett agerande av en person som personen kan kontrollera och som därmed är beroende av personens skäl, motiv, avsikter och liknande.[121] Begreppet *följd* åsyftas det resultat som inträffar till följd av handlingen. Slutligen innebär begreppet *omständigheter* de fakta som omgärdar gärningstillfället.

Det anses idag finnas tre former av uppsåt, avsikts-, insikts- och likgiltighetsuppsåt, men det ställs inga krav på vilken grad av uppsåt som krävs för att kunna hållas personligt ansvarig för ett brott.[122]

[120] Asp, Ulväng och Jareborg, s. 285.
[121] Asp, Ulväng och Jareborg, s. 74.
[122] Det krävs i vissa fall att det föreligger så kallat överskjutande uppsåt exempelvis för stöld (BrB 8:1) där det krävs att personen har ett uppåt att ”tillägna” sig föremålet för att ansvar ska kunna utkrävs. Dock prövas i dessa fall det överskjutande uppsåtet inte i steget för personligt ansvar utan i steget där otillåten gärning prövas eftersom det anses vara en del av gärningsbeskrivningen. Se Asp, Ulväng ch Jareborg s. 361 samt s. 60.

6.2.3.1. Vad ska uppsåtet omfatta? (Täckningsprincipen)

För personligt ansvar krävs alltså att gärningspersonen haft uppsåt till den otillåtna gärningen, vilket innebär att gärningspersonens uppsåt ska ha varit riktat mot varje föreskrivet rekvisit vid gärningstillfället och till avsaknaden av rättfärdigande omständigheter vid tidpunkten.[123]

Uppsåt behöver dock inte föreligga från början till slut utan det räcker med att gärningspersonen haft uppsåt under slutdelen av gärningen, exempelvis om någon först av misstag tar någon annans portfölj men efter upptäckten ändå väljer ta med sig portföljen hem.[124] Uppsåtet kan inte heller ha uppstått efter händelsen eller förelegat innan händelsen men upphört innan tidpunkten för handlingen.[125]

Uppsåtet ska således täcka rekvisiten för gärningsbeskrivningen vid tidpunkten varför denna princip kallas *täckningsprincipen*.

6.2.4. Ursäktande omständigheter

Det sista steget att kontrollera är om det finns ursäktande omständigheter. Om det finns ursäktande omständigheter innebär det att gärningspersonen trots att gärningen är otillåten och att gärningspersonen haft uppsåt till den kan undgå personligt ansvar. Ett sådant fall är om personen ifråga har handlat under tillfällig sinnesförvirring eller straffrättsvillfarelse (BrB 24:9).[126] Detta innebär att en person kan ursäktas för en egentligen brottslig gärning på grund av vissa exceptionella omständigheter.

[123] Asp, Petter och Ulväng, Magnus, *Täckningsprincipens ABC*, Juridisk publikation Nummer 02/2009, [s. 265-273], Stockholm, 2009, s. 271, http://juridiskpublikation.se/wp-content/uploads/2014/10/22009_Petter-Asp-Magnus-Ulv%C3%A4ng.pdf.
[124] Asp, Ulväng och Jareborg, s. 325-326.
[125] Asp, Ulväng och Jareborg, s. 295.
[126] Asp, Ulväng och Jareborg, s. 370 ff.

6.2.5. Har ett brott begåtts?

När samtliga steg har gåtts igenom har vi en slutsats angående om ett brott har begåtts. I korthet:

1) Är gärningsbeskrivningsenlighet uppfyllt,
2) har gärningspersonens handlande inte var rättfärdigat och har gärningspersonen inte heller trott att handlingen var rättfärdigad,

----------**Otillåten gärning**----------

(Ansvar för medverkan kan här uppkomma.)

3) har gärningspersonen haft uppsåt till sitt handlande, följderna samt omständigheterna vid tidpunkten för den otillåtna gärningen och,
4) saknas det ursäktande omständigheter för gärningspersonens handlande,

kan det slutligen konstateras att ett brott har begåtts som gärningspersonen är personligt ansvar för och ska då även åläggas ett straff.

6.2.6. Oaktsamhet

Avslutningsvis i denna del ska något sägas om oaktsamhet. Oaktsamhetsbegreppet används inom straffrätten i två olika hänseenden. I det ena fallet åsyftas personens inställning till en otillåten gärning, alltså personens okunnighet eller villfarelse om att en otillåten gärning fullbordas.[127] Det är i detta fall det personliga ansvaret kan inträda trots att personen saknat uppsåt. Det andra fallet är när en person handlat på ett oaktsamt eller vårdslöst sätt som det heter i lagtext, vållande till annans död är ett exempel på ett sådant brott.[128] Den oaktsamhet som kommer beröras här är den oaktsamhet som kan leda till personligt ansvar, alltså gällande gärningspersonens inställning.

För att kunna bli personligt ansvarig för sin oaktsamhet krävs att det är särskilt föreskrivet för det specifika brottet att det räcker att gärningspersonen varit oaktsam i förhållande till den otillåtna gärningen i motsats till huvudregeln uppsåt.

En person kan vara antingen *medvetet* eller *omedvetet* oaktsam. Medveten oaktsamhet innebär att personen uppfattar att det är sannolikt att en viss följd inträffar eller omständighet föreligger och att gärningspersonen är likgiltig inför *risken* följden eller omständigheten. Om

[127] Asp, Ulväng och Jareborg, s. 178.
[128] BrB 3:7.

gärningspersonen istället är likgiltig inför att själva *resultatet* rör det sig istället om ett så kallat likgiltighetsuppsåt.

Omedveten oaktsamhet innebär att gärningspersonen haft *skälig anledning att anta* eller *borde ha förstått* att en viss följd skulle inträffa eller att en viss omständighet förelåg men inte gjorde det. Prövningen av omedveten oaktsamhet görs genom att i första ledet pröva vad gärningspersonen *kunde ha gjort* för att komma till insikt exempelvis om personen hade kunnat tänka efter, vara uppmärksam, inhämta information eller skaffa hjälp för att hitta information. Sedan prövas om personen hade *förmåga och tillfälle* att komma till *insikt*, denna prövning görs med utgångspunkt i den enskilda personens förmåga.[129] I andra ledet prövas om gärningspersonen *borde* ha vidtagit de åtgärder som hade kunnat krävas för att komma till insikt,[130] detta är en normativ prövning av om handlingarna i första ledet rimligen borde ha vidtagits.[131]

[129] Det så kallade ”orsaksledet”, Asp, Ulväng och Jareborg, s. 315.
[130] Det så kallade ”klandervärdhetsledet”, Asp, Ulväng och Jareborg, s. 315.
[131] Asp, Ulväng och Jareborg, s. 316 f.

7. 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 faktiskt och inte bara tekniskt. I denna rapport baseras redogörelsen enkelt uttryckt på att tillhandahållande av Tor-noder anses innebära ett tillhandahållande av verktyg för att skapa anonymitet för användare.

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 lånat 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.

7.1. 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 är ett brott att försvåra identifiering av någon som begår brott.

Det brott som ligger närmast till hands är *skyddande av brottsling* enligt BrB 17:11:

> ”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.
>
> För skyddande av brottsling döms också den som undanröjer bevis om brott som är föremål för ett rättsligt förfarande vid Internationella brottmålsdomstolen eller på annat dylikt sätt motverkar att det uppdagas eller beivras.
>
> Är brottet grovt, döms till fängelse, lägst sex månader och högst fyra år.
>
> Den som inte insåg men hade skälig anledning att anta att den andre var brottslig, döms till böter.
>
> Ansvar ska inte dömas ut om gärningen är att anse som ringa med hänsyn till gärningsmannens förhållande till den brottslige och övriga omständigheter”

Brottet kan enligt brottsbeskrivningen begås antingen genom att dölja gärningspersonen eller genom att dölja själva brottet.

Döljande av brott är exempelvis att avlägsna spår från en gärningsplats såsom finger- eller fotavtryck.[132] Döljande av gärningspersonen innebär att motverka att brottet upptäcks eller att gärningspersonen upptäcks, blir föremål för utredning, lagföring, dom eller verkställighet av straff.[133]

För att bli personligt ansvarig krävs inte enbart uppsåt till att en annan person begått ett brott utan också att den egna handlingen som vidtagits skett i syfte att dölja brott eller försvåra utredning och lagföring.[134]

I BrB 17:11 st. 4 föreskrivs dessutom att det räcker med att en person varit oaktsam (*inte insåg men hade skälig anledning att anta*) i förhållande till att en person begått ett brott. 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.[135]

Enligt bestämmelsen krävs det att döljandet sker efter det att ett brott har begåtts. Tillhandahållande av Tor-noder möjliggör anonymisering för användare undertiden de utför brott över internet. Efter det att en användare utfört ett brott samtidigt som den använt Tor sker ingen åtgärd från tillhandahållaren för att dölja brottslingen. Tillhandahållare av Tor-noder möjliggör därför bara anonymitet under den tid användaren begår brottet och bör därför inte kunna hållas ansvarig för skyddande av brottsling enligt BrB 17:11. Däremot skulle tillhandahållare av Tor-noder eventuellt kunna hållas ansvarig för medverkan vilket kommer att beröras i avsnitt 8.

7.2. Uppvigling

En annan fråga som kan uppkomma är om tillhandahållande av Tor-noder är en sådan uppmuntran till otillåten gärning att den inryms i begreppet uppvigling i BrB 16:5.

För fullbordan av detta brott krävs att gärningspersonen *söker föranleda brottslig gärning* och att uppmanandet är riktat till allmänheten. Ett meddelande publicerat på internet har ansetts

[132] Nilsson, Göran, *Brottsbalk (1962:700) 17 kap. 11 §*, Lexino 2015-08-01, 2.2.3.
[133] Nilsson, BrB 17:11 2.2.4.
[134] Nilsson, 2.4.1.
[135] Nilsson, BrB 17:11, 2.2.4.

vara ett meddelande till allmänheten enligt brottsbeskrivningen.[136] Det krävs dock att uppmaningen sker via ett *meddelande*. Det krävs alltså att den som uppviglar gör detta genom ett budskap. Att konfigurera en enhet kan i sig inte anses utgöra ett meddelande innehållande budskap enligt lagens mening, även om noden blir synlig i consensus såsom beskrivits i avsnitt 1.1.2.

Tillhandahållare av Tor-noder ska därför inte anses kunna åläggas ansvar för uppvigling enligt BrB 16:5.

7.3. Summering

Tillhandahållande av Tor-noder bör inte anses kunna utgöra skyddande av brottsling enligt BrB 17:11 eftersom den anonymitet som Tor möjliggör bara föreligger under tiden användaren begår ett brott via internet. För att skydda en brottslig krävs att skyddet ges efter det att ett brott har begåtts. Det bör således konstateras att tillhandahållande av Tor-noder troligen inte ska anses utgöra skyddande av brottsling enligt BrB 17:11.

Inte heller bör tillhandahållande av Tor-noder kunna anses utgöra uppvigling enligt BrB 16:5 eftersom tillhandahållandet av Tor-noder saknar den förmedling av meddelande med innehåll till användarna som krävs enligt bestämmelsen.

Det ska alltså inte anses föreligga någon brottbeskrivningsenlighet för dessa två huvudbrott vid tillhandhållande av Tor-noder. Av de brott som återfinns i BrB och i specialstraffrätten är det dessa två brott som närmast skulle kunna ligga till hands varför redogörelsen endast har gjorts av dessa två.

[136] Nilsson, 16:5, 777).

8. Medverkan

Det krävs generellt inget särskilt stadgande för att medverkan till brott ska vara straffbart, det krävs inte heller att gärningspersonen har identifierats för att personligt ansvar för medverkan ska uppkomma.[137] 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.[138] I The Pirate Bay-domen (”TPB-domen”)[139] konstaterade Svea hovrätt exempelvis att det var styrkt att det fanns gärningspersoner men att dessa var okända.[140] Medverkan kan även ske till straffbelagd förberedelse, försök, stämpling och medverkan till brott, alltså är det möjligt att straffas för medverkan till medverkan.[141]

Medverkan till brott finns i BrB 23:4:

> ”Ansvar som i denna balk är föreskrivet för viss gärning skall ådömas inte bara den som utfört gärningen utan även annan som främjat denna med råd eller dåd. Detsamma skall gälla beträffande i annan lag eller författning straffbelagd gärning, för vilken fängelse är föreskrivet.
>
> Den som inte är att anse som gärningsman döms, om han har förmått annan till utförandet, för anstiftan av brottet och annars för medhjälp till det.
>
> Varje medverkande bedöms efter det uppsåt eller den oaktsamhet som ligger honom till last. Ansvar som är föreskrivet för gärning av syssloman, gäldenär eller annan i särskild ställning skall ådömas även den som tillsammans med honom medverkat till gärningen.
>
> Vad som sägs i denna paragraf skall inte gälla, om något annat följer av vad för särskilda fall är föreskrivet.”

Enligt första stycket krävs det alltså för medverkan till ett brott inom specialstraffrätten att fängelse finns med i straffskalan för brottet.

Medverkanspersonens handlingar eller underlåtenhet ska prövas på samma sätt som beskrivits i 6.2 men prövningen görs i förhållande till om ett huvudbrott främjats istället för om ett

[137] Asp, Ulväng och Jareborg, s. 430.
[138] Asp, Ulväng och Jareborg, s. 436, det kan alltså ha förelegat en rättfärdigande omständighet för huvudgärningspersonen varför denne kan undgå ansvar samtidigt som en annan person kan hållas ansvarig för medverkan.
[139] Mål nr B 4041-09, Svea Hovrätt, 2010-11-26.
[140] TPB-domen, s. 17.
[141] Asp, Ulväng och Jareborg, s. 425.

huvudbrott har blivit begånget. Medverkanspersonens ansvar bedöms alltså enskilt från gärningspersonens, vilket i sin tur innebär att medverkanspersonen kan bli ansvarig för medverkan till ett annat brott än det som huvudgärningspersonen blir dömd för. Exempelvis om en person dödats och gärningspersonen haft uppsåt till mord medan medgärningspersonen endast haft uppsåt till misshandel döms medgärningspersonen för medhjälp till misshandel.[142] 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.[143]

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.[144] Det ställs alltså likt ovan beskrivet krav på kausalitet mellan medverkanspersonens påverkan och gärningspersonens gärningar.

Första steget i bedömningen blir likt systematiken för prövning av gärningspersonens handlingar att se om medverkanspersonens agerande främjat något föreskrivet brott. Främjandet kan ske både genom att medverkanspersonen utför en handling eller genom att underlåta att göra något. Alltså om medgärningspersonen har främjat gärningspersonens otillåtna gärning.[145] För att kunna göra detta behöver det så kallade medverkansobjektet utkristalliseras. Medverkansobjektet utgörs av gärningspersonens otillåtna gärning eller gärningar.[146] Om det kan konstateras att en brottsbeskrivningsenlighet föreligger för gärningspersonens handling och det saknas rättfärdigande omständigheter kan det prövas om medverkanspersonen har främjat medverkansobjektet trots att gärningspersonen ännu inte är identifierad. Det krävs alltså bara att gärningspersonen gjort 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 åläggas en medverkansperson.

Någon 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

[142] Asp, Ulväng och Jareborg, s. 437.
[143] NJA 2007 s. 929.
[144] Nicander, Hans, *Upphovsrätten och medverkansansvaret i en digital miljö*, SvJT 2012 [258-281] s. 260.
[145] Asp, Ulväng och Jareborg, s. 430.
[146] Asp, Ulväng och Jareborg, s. 436.

garantställning[147].[148] Tillhandahållare av Tor-noder kan inte anses ha granatställning enligt hur ansvaret har utformats, varför medverkansansvar genom underlåtenhet inte kommer att beröras närmare i denna rapport.[149]

Det bör återigen påminnas om att de som mest sannolikt skulle kunna bli föremål för misstanke om medverkan är de som tillhandahåller utgångsnoder i och med att det är deras ip-adresser som är synliga på de besökta hemsidorna eller står som avsändare av meddelanden.

Medverkan är i BrB 23:4 uppdelat i två former: 1) anstiftan och, 2) medhjälp. Anstiftan skulle enkelt kunna jämföras med beställning av ett brott medan medhjälp mer liknar assistans till utförandet av ett brott.

8.1. Anstiftan

Anstiftan 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.[150] En straffbar anstiftan förutsätter att anstiftaren hos en annan person framkallat beslut att begå brott, det krävs alltså en form av psykiskt 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.[151] 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[152] eller att uppdra åt någon att genomföra ett brott samt lämna nödvändig information för att brottet skulle kunna fullbordas[153]. Det som är gemensamt för målen om anstiftan är att det har skett en korrespondens mellan medverkanspersonen och gärningspersonen (eller ett led till denne) där information om vilken handling eller vilket resultat som den otillåtna gärningen ska utgöra. Det psykiska sambandet bör alltså anses innefatta någon form av reell uppfattning om vad som ska ske och ska förmedlas mellan personerna.

[147] Exempelvis vårdnadshavare eller badvakt, se även BrB 23:6.
[148] Se även NJA 2003 s. 473 för vidare resonemang.
[149] SOU 1996:185, *Straffansvarets gränser Del 1, Betänkande från Straffansvarsutredningen*, s. 311 ff.
[150] Asp, Ulväng och Jareborg, s. 441.
[151] Zila, Josef, *Brottsbalk (1962:700) 23 kap. 4 §*, Lexino 2012-07-01, 2.3.1.
[152] Se tingsrättens resonemang i NJA 1999 s. 561.
[153] RH 2015:40, Svea hovrätt, 2015-03-05.

Tillhandahållare av Tor-noder står inte i någon kontakt med användarna av Tor annat än att deras enheter korresponderar. Det förmedlas inte heller genom tillhandahållandet av Tor-noder någon information till användarna om vad tillhandahållarna vill att användarna ska göra eller för den delen vad användarna vill göra. Genom bristen på innehållsmässig korrespondens 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. Med innehållsmässig korrespondens menas i denna rapport korrespondens där en person har möjlighet att utläsa ett meddelande av något slag som inte endast är teknisk data såsom källkod eller liknande.

Saken blir naturligtvis en annan om en tillhandahållare av Tor-noder uttryckligen ber någon att koppla upp sig mot dennes nod för att begå ett visst brott, men då föreligger det även innehållsmässig korrespondens mellan tillhandahållaren och användaren vilken är fristående från tillhandahållandet av Tor-noder.

Erbjudandet av 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 bör anses kunna anstifta någon att begå ett brott även om tillhandahållande av anonymitet skulle påverka vissa användares handlande.

8.2. Medhjälp

Medhjälp innebär att medverkanspersonen psykiskt till exempel genom råd eller uppmuntran eller fysiskt genom att tillhanda hjälpmedel för utförandet av den otillåtna gärningen 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.[154] Medhjälp kan se både genom psykiskt och fysisk främjande enligt lagtextens formulering ”råd” (psykiskt) eller ”dåd” (fysiskt).

Eftersom lagtexten tar sikte på att någon försöker underlätta att ett brott utförs omfattas även handlingar som i verkligheten inte underlättar utförandet av brottet eller tillochmed försvårar utförandet av det så länge medverkanspersonens handlande har varit ett försök att

[154] Zila, 23:4, 2.3.2.

underlätta.[155] Medverkanspersonens påverkan kan tillochmed vara relativt obetydligt för att det ändå ska anses som ett främjande.[156] Exempel på medhjälp har ansetts vara att hålla en jacka för att någon annan ska kunna misshandla någon (har ansetts stärka gärningspersonens uppsåt, alltså psykiskt),[157] att stanna en bil för att låta personerna i bilen misshandla ett annat gäng när föraren kände till att de redan tidigare under kvällen misshandlat det andra gänget,[158] och att hålla vakt vid ett inbrott.[159]

Gränsen för vad som räknas som ett straffbart främjande är ställt lågt 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.”.[160] 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 kunna göra en bedömning.[161]

8.2.1. Psykiskt främjande av brott genom tillhandhållande av Tor-noder

Att styrka gärningspersonen i dennes uppsåt är att betrakta som ett psykiskt främjande och 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 statistik eller andra uppgifter om att personer skulle bli mer benägna att begå brott via internet genom användningen av Tor.

Ändå bör frågan om möjligheten till anonymitet kan anses vara en uppmuntran eller ett råd till någon i lagens mening beröras.

Det har inte ansetts som främjande att gillande bevittna en misshandel eller liknande utan det krävs att medverkanspersonen aktivt påverkar händelseförloppet enligt förarbetena.[162] HD ansåg i ett fall att en person som suttit med i en bil när två andra personer skjutsats till och från en plats för att utföra en misshandel och gått ut ur bilen för att delvis bevittna det inte gjort sig skyldig till medhjälp eftersom personen i så hög grad stått utanför

[155] Asp, Ulväng och Jareborg, s. 438.
[156] Asp, Ulväng och Jareborg, s. 438.
[157] NJA 1963 s. 574.
[158] NJA 1984 s 922.
[159] NJA 2006 s. 577.
[160] SOU 1944:69, *Lagstiftning om brott mot staten och allmänheten*, s. 91.
[161] Asp, Ulväng och Jareborg, s. 439.
[162] SOU 1996:185, s. 189.

händelseförloppet.[163] För att det ska vara fråga om psykiskt främjande torde det enligt praxis och förarbeten krävas att någon exempelvis hejar på någon vid ett slagsmål eller ger tips om hur en person lättast skadas genom ett knytnävsslag.

Om en person som tvekar inför att begå ett brott beslutar sig för att skrida till verket på grund av att denna känner sig skyddad av anonymiteten som Tor-nätverket medger, innebär det de facto att en person övertygas om att begå ett brott. Genom att tillhandahålla Tor-noder skulle det i det fallet kunna argumenteras för att tillhandahållarna psykiskt påverkar dessa användare att begå brott. Alltså att tillhandahållarna på något sätt ”styrker gärningspersonerna i deras uppsåt” genom att tillhandahålla Tor-noder. För att hållas ansvarig för medhjälp krävs dock som beskrivits att medverkanspersonens främjande rör huvudbrottet. Eftersom tillhandahållare av Tor-noder varken korresponderar med användarna eller får någon information om när användarna använder deras noder eller vad användarnas trafik är tänkt att gå till 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.

Skulle en tillhandahållare av Tor-noder istället lämna råd om hur en person kan agera för att till exempel hitta en hemsida eller vad en person kan göra i skydd av anonymitet skulle psykisk påverkan kunna föreligga.

Det bör därför kunna konstateras att endast tillhandahållande av Tor-noder inte bör kunna anses utgöra medhjälp genom psykiskt främjande enligt BrB 23:4.

8.2.2. Fysiskt främjande av brott genom att tillhandahålla anonymitet

Fysiskt främjande kräver att det tillhandhålls ett hjälpmedel som är avsedda att underlätta utförandet av själva brottet. Att skapa anonymitet kan inte anses underlätta utförandet av brott

[163] NJA 1984 s. 922.

eller vara ägnat att underlätta[164] eftersom det är identifieringen av den som begår brottet som försvåras.

Dock ges i förarbeten och doktrin exempel på medhjälp i form att en person vaktar medan en eller flera andra gör ett inbrott. Att hålla vakt kan förvisso inte heller tyckas vara ett direkt underlättande av utförandet av brottet utan snarare ett sätt att förhindra upptäckten av brott, men kan även ses mer som en psykisk påverkan i form av uppmuntran. Det kan också baserat på förarbeten och doktrin anses som att hålla vakt vid ett inbrott medger att medverkanspersonen kan påverka händelseförloppet eftersom medverkanspersonen då befinner sig på platsen för brottet.

Frågan om ansvar för medhjälp i digitala miljöer har under senare år aktualiserats mer och mer,[165] redan 1996 i den så kallade BBS-domen[166] berörde HD frågan ytligt. HD kunde dock inte pröva frågan om medverkan på grund av utformningen av åklagarens ansvarspåståenden och fortfarande idag har frågan inte prövats av HD. Däremot prövades frågan i TPB-domen där Svea hovrätt hänvisade till BBS-domen i sitt resonemang. Svea hovrätt prövade om tillhandahållarna av fildelningshemsidan The Pirate Bay (”TPB”) gjort sig skyldiga till medverkan till upphovsrättsbrott enligt 53 § upphovsrättslagen[167].

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.[168] Svea hovrätt ansåg alltså att de funktioner som erbjöds genom TPB utgjorde en sådan tjänst som underlättade de upphovsrättsbrott som användarna utförde på hemsidan.

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.

---

[164] SOU 1996:185, s. 187.
[165] Se bl.a. Mål nr B 3117-13, Svea hovrätt, 2013-10-31, om medverkan till upphovsrättsbrott och Mål nr B 2932-16, Svea hovrätt, 2016-03-30, om medverkan till bedrägeri.
[166] NJA 1996 s. 79, om en tillhandahållande av BBS (Bulletin Board System) kunde åläggas ansvar för upphovsrättsbrott enligt 53 § 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.
[167] Lag om upphovsrätt till litterära och konstnärliga verk (SFS 1960:729).
[168] TPB-domen, s. 24.

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.

I ett annat mål från Svea hovrätt (”hubb-domen”) angående medhjälp till upphovsrättsbrott dömdes en person för att ha tillhandahållit en så kallad DirectConnect-hubb.[169] 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.[170] 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 6.2.3.1.

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, men där slutar också likheterna mellan hubb-domen och tillhandahållandet av Tor-noder.

Eftersom tillhandahållande av anonymitet varken direkt eller indirekt främjar de brott som kan begås via internet skulle en argumentationslinje för att tillhandahållande av Tor-noder skulle främja brott på ett sådant sätt som omfattas av begreppet medhjälp slå fel.

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

[169] Mål nr B 3117-13, Svea hovrätt, 2013-10-31.
[170] Mål nr B 3117-13, Svea hovrätt, 2013-10-31, s. 5.

form av exempelvis hemsidor 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.

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.[171] Står en person för långt utanför händelseförloppet kan denne inte anses främja brottet. Hade tillhandahållare av Tor-noder behövt godkänna all trafik som går genom deras noder hade de haft påverkan på händelseförloppet, eller om de hade haft möjlighet att bara dirigera trafik till sidor med olagligt material skulle tillhandahållare av Tor-noder kunna anses vara medhjälpare till gärningspersoner, men det är inte så Tor idag fungerar.

Möjliggörande av anonymitet via Tor bör därför inte i sig kunna utgöra ett främjande enligt lagens mening även om identifieringen av gärningspersonen försvåras.

8.2.3. Fysiskt främjande av brott att tillhandahålla bandbredd

Tillhandahållare av Tor-noder tillgängliggör som beskrivits i 1.1.3 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.[172] 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 menig 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 innebär att även mindre 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 slutmålet och dels att användarna kan dölja sig bakom tillhandahållarnas ip-adresser. Användarna av Tor-nätverket behöver dock själva ha tillgång

[171] Asp, Ulväng och Jareborg, s. 40.
[172] TPB-domen, s. 30.

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 alltså 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 som 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.[173] 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 tillhandahållandet av bandbredden 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 såsom redogjorts för i avsnitt 6.2.3 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 om medverkanspersonen haft uppsåt till sin egen handling och dels om medverkanspersonen haft uppsåt till huvudgärningen.[174] I fråga om Tor innebär det dels att tillhandahållaren behöver ha uppsåt till att tillhandahållandet är ett främjande av huvudgärningen samt att huvudgärningen utförs.

Som tidigare påpekats finns det ingen statistik eller bekräftade uppgifter om vad användarna av Tor gör när de utnyttjar tjänsten, tillskillnad från TPB där tillhandahållarna vid flera tillfällen uppmärksammats på att det begicks upphovsrättsintrång och dessutom mottog varningsbrev och liknande om saken.[175]

[173] TPB-domen, s. 34.
[174] NJA 2003 s. 473.
[175] TPB-domen, s. 25.

Tillhandahållarna av TPB behövde alltså inte har någon direkt korrespondens med gärningspersonerna för att få kännedom om att det begicks brott på TPB utan det räckte med att de fått kännedom om användarnas gärningar. Det krävdes alltså kännedom om typen av otillåten gärning för att tillhandahållarna av TPB skulle kunna hållas ansvariga.[176] 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 utan det krävs viss kännedom om ett visst förhållande eller typ av handling utan att händelseförloppet stämmer exakt överens med medhjälpspersonens bild av händelsen.[177]

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.[178]

Tillhandahållare av Tor-noder tillhandahåller anonymitet till de som vill läsa nyheter på internet likväl som till de som vill skicka och ta emot barnpornografi. Själva tjänsten som tillhandahållare av Tor-noder möjliggör ger inte på så sätt som i TPB-domen någon indikation om användarnas handlingar och denna information kan tillhandahållarna av Tor-noder inte heller genom tillhandahållandet förvärva.

Det bör här dock nämnas att Tor och användingen av Tor ofta av allmänheten många gånger förknippas med brottsliga aktiviteter. ”Deep web”[179] är något som ofta dyker upp i diskussioner om Tor. ”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. Stora delar av ”Deep web” består av precis samma typ av innehåll som det indexerade-internet består av, alltså hemsidor med bilder, text och liknande. Att material finns på ”Deep web” är inte heller alltid ett val som avsändaren av materialet har valt utan det kan bero på tekniska skäl som gör att sökmotorerna inte indexerar alla filtyper och liknande som läggs upp varför innehållet endast blir tillgängligt om hela adressen skrivs in i adressfältet i webläsaren.

Vid sökningar på internet förekommer det ett antal sökträffar där användning av Tor rekommenderas för användare som vill tillgå ”Deep web” inte i första hand för att skydda användares identitet vid utförandet av eventuella brott utan för att skydda användare mot att bli föremål för brottsliga gärningar. Det bör anses vedertaget att det på ”Deep web” döljer sig brottslig aktivitet på samma sätt som det på det indexerade internet förekommer brottslig

[176] TPB-domen, s. 41.
[177] TPB-domen, s. 27.
[178] TPB-domen, s. 23 f.
[179] Wikipedia om Deep web, https://sv.wikipedia.org/wiki/Deep_web.

aktivitet. Hur stor omfattning det sker i saknas det idag uppgifter om likt det saknas 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.

Termen ”Darknet”[180] förekommer också i samband med Tor-nätverket. Tor-nätverket anses utgöra ett ”Darknet”. Namnet till trots innebär ”Darknet” egentligen bara att användare behöver en viss typ av mjukvara för att få tillgång till det nätverk de vill träda in i. I fallet med Tor innebär det exempelvis 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.

När tillhandahållarna av Tor-noder konfigurerat sina enheter och underhåller noderna med el och internetanslutning har de vetskap om att deras noder närsomhelst och 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.

Även om Tor figurerat i media i samband med brottsliga aktiviteter exempelvis gällande ”Silk road”,[181] finns det idag inga direkta bevis för att en stor del av trafiken i Tor är kopplad till brottslig verksamhet på det sätt som framgick i TPB-domen. Det kan därför inte anses vara vedertaget att Tor i huvudsak används för brottsliga gärningar och tillhandahållarna kan inte anses ha sådan kännedom om brottslig aktivitet baserat på tjänstens karaktär eller hur användarna väljer att utnyttja den att de skulle kunna innebära uppsåt till brott.

Om exempelvis Polisen skulle höra av sig med uppgifter om att en tillhandahållen Tor-nod för närvarande utnyttjas för att besöka en hemsida för barnpornografi skulle det dock kunna anses som att tillhandahållaren uppnått sådan kännedom om brottet att tillhandahållaren skulle kunna hållas straffrättsligt ansvarig för medhjälp om denne då inte stänger av sin enhet.[182]

Ansvaret för tillhandahållare av Tor-noder skulle enligt exemplet kunna jämföras med ISP:ers ansvar i vissa fall. ISP:er kan exempelvis enligt Infosoc-direktivet åläggas medverkansansvar för upphovsrättsintrång om ISP:n får konkreta indikationer på att deras serverutrymme

[180] Wikipedia om Darknet, https://sv.wikipedia.org/wiki/Darknet.
[181] FBI stängde ökänd drog- och vapenhandelssajt, Bie Nanok, 2 oktober 2013, uppdaterad 9 oktober 2013, http://www.svt.se/nyheter/utrikes/okanda-drog-och-vapenhandelssajten-silk-road-nedstangd.
[182] Denna situation bör dock inte anses innebär ett underlåtenhetsansvar som innebär att tillhandahållaren påförs en garantställning för tillhandahållandet av tjänsten.

används på ett sätt som innebär upphovsrättsintrång men inte agerar på denna informationen. Däremot är medverkansansvaret inte straffrättsligt utan civilrättsligt eftersom juridiska personer inte kan begå brott. Frågan om ISP:ers ansvar har prövats i Stockholms tingsrätt.[183] I det fallet ansågs inte ISP:n ha medverkat till upphovsrättsbrott trots att de hade kännedom om att det bland annat på TPB begicks upphovsrättsbrott och att trafik genom deras tjänst gick till hemsidan. Anledningen var att det var en så liten del av all trafik som gick till dessa sidor och att ISP:n inte själv hade något avtal med tillhandahållarna av tillhandahållarna av tjänsterna. Denna dom är dock överklagad till Svea hovrätt som kan komma att ändra på hur frågan ska tolkas.

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. Detta är dock i slutändan en bevisningsfråga som en domstol behöver ta ställning till likt i TPB-domen.

Tillhandahållare av Tor-noder bör därför inte anses kunna hållas ansvariga för medhjälp på grund av tillhandahållande av Tor-noder.

8.3. Oaktsam medverkan

För att oaktsam medverkan ska vara straffbar krävs att även oaktsamhet för huvudbrottet är straffbart.[184] Oftast döms den som genom oaktsamhet medverkat till ett brott själv för det oaktsamma huvudbrottet.

Det finns flera brott, bland annat vissa former av barnpornografibrott och upphovsrättsbrott där oaktsamhet eller grov oaktsamhet räcker för att hållas ansvarig. En revisor hölls i en dom från HD ansvarig för oaktsam medverkan när denne noterat att boksluten för ett bolag hade inneburit ovanligt stora arbetsinsatser för kollegorna som arbetade med ärendet men inte kontrollerat saken närmare. HD ansåg att revisorn borde ha kontrollerat varför ärendet upptog en så stor arbetsinsats.[185] Som beskrivits i 6.2.6 finns det även två typer av oaktsamhet som båda kan leda till ansvar och i fallet från HD rörde det sig om omedveten oaktsamhet.

[183] Mål nr T 15142-14, Stockholms tingsrätt, 2015-11-27.
[184] SOU 1944:69, s. 94.
[185] NJA 1988 s. 383.

I stora drag skulle alltså en tillhandahållare av Tor-noder antingen behöva uppfatta att det är sannolikt att en viss huvudgärning inträffar om Tor-noderna tillhandahålls och att tillhandahållaren är likgiltig inför risken att huvudgärningen inträffar, eller 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-noder.

Båda dessa fall kräver alltså att tillhandahållaren ska ha någon form av uppfattning eller borde ha någon forma 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 den första formen av oaktsam medverkan, 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.

Den första frågan blir om tillhandahållare av Tor-noder kunde ha gjort något för att komma till insikt exempelvis vara uppmärksam, inhämta information eller skaffa hjälp för att hitta information. En 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 starta skadliga Tor-noder och utföra vidare steg. Enkelt uttryckt är det svårt och krångligt att göra det eftersom Tor är uppbyggt för att det inte ska gå att spåra trafiken. Av de sökningar och intervjuer som gjorts framgår att ingen har fullständig kännedom om hur detta görs och ingen vill heller försöka eftersom detta skulle påverka Tor-nätverket negativt.[186]

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 framstår att få information om trafiken i Tor-nätverket måste det anses som 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 i den första frågan betonats är det väldigt svårt att ta reda på denna information och det krävs omfattande

[186] Mejlkonversation med utvecklare av Tor samt tillhandahållare av Tor-noder.

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 som att det är 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 nod 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 var den går. Det är i nästa led ännu svårare att ta reda på om det faktiskt finns en fysisk person bakom klienten.

8.4. Social adekvans

Innan uppsåt eller oaktsamhet prövas ska dock som redogjorts i 6.2.2 frågan om det föreligger några rättfärdigande omständigheter prövas.

Det kan inte anses föreligga något nödvärn, nöd eller samtycke för döljandet av någons identitet genom tillhandahållandet av Tor-noder om användaren begår brott. Tillhandahållandet skulle dock 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 som: typen av risk, vilka värden riskerna riktar sig mot, själva gärningens sociala värde samt vilka försiktighetsåtgärder som varit möjliga och befogade att vidta.[187] Bedömningen ska enligt hovrättens resonemang alltså göras av om tjänsten som tillhandahålls kan anses vara tillräckligt värdefull eller viktig i allmänhet samtidigt som de oönskade

[187] 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.”.

riskerna är proportionerliga i förhållande till värdet av tjänsten, för att döljandet av brottslingar ska anses vara socialt adekvat vid tillhandahållande att tjänsten. Svea hovrätt nämnde 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.[188] I dessa fall borde social adekvans kunna användas som rättfärdigande omständighet.

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 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.[189]

I fråga om tillhandahållande av Tor-noder finns det idag ingen statistik på hur många av användarna som begår brott när de använder sig av Tor, såsom berörts i 8.2.3. 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 idag inte heller någon statistik över hur ofta brott begås över internet i sin helhet eller per nation, dock har rättsväsendet i flertalet länder noterat att brott som begås genom användande av internet ökar årligen.

Om det skulle gå att klarlägga att möjligheten till anonymitet har en tilldragande effekt för personer som vill begå brott genom internet skulle detta kunna inverka på bedömningen och då anses ”mindre” rättfärdigat att tillhandahålla Tor-noder då proportionerna skulle förskjutas. Det skulle dock krävas att det rörde sig om en stor grupp personer och att frekvensen av begångna brott vid användandet av Tor var klarlagd och hög. Det skulle även kunna anses ”mer” oproportionerligt om tjänsten marknadsfördes eller riktade sig till personer som ville

[188] TPB-domen, s. 24.
[189] TPB-domen, s. 25.

dölja sin kriminalitet. Det går dock att fastslå att Tor och liknande tjänster främst marknadsförs mot personer, företag och organisationer som vill vara anonyma på internet i syfte att skydda sig själva från integritetsintrång eller skydda sin kommunikation i lagliga syften, exempelvis företagshemligheter.

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 riktad till personer som vill dölja sin brottslighet, tvärtom marknadsförs Tor som ett sätt att stärka skyddet för personers integritet och yttrandefrihet. Dessa värden torde anses vara av stor vikt och anses värdefulla i ett samhälle. Dessa intressen är även uttryckligen grundlagsskyddade både nationellt och genom EU:s rättighetsstadga[190]. 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 at begå brott.

8.5. Strafflättnad BrB 23 kap. 5 §

Skulle tillhandahållande av Tor-noder anses utgöra medverkan som leder till straffrättsligt ansvar för medverkan[191] finns det möjlighet för den som bara i mindre utsträckning medverkat till ett brott att få sitt straff sänkt under straffminimum eller helt undgå ansvar. För att strafflättnadsregeln ska kunna användas krävs det att flera personer medverkat till brottet eftersom bedömningen görs i jämförelse med de övriga medverkandes handlingar.[192] Om varje tillhandahållare av Tor-noder i en dirigeringskedja skulle anses medverka till brott skulle denna regel kunna vara tillämplig, eller om både tillhandahållare av Tor-noder och den som tillhandahållit någon annan tjänst som främjat huvudbrottet skulle anses medverka till brott.

Strafflättnaden ges i förhållande till det *straffvärde* som medverkanshandlingen anses utgöra. Straffvärde är ett mått på hur allvarlig lagstiftaren tycker att handlingen är.[193] I TPB-domen ansågs strafflättnadsregeln inte vara tillämplig eftersom upphovsrättsbrott genom fildelning enligt Svea hovrätt utgjorde ett samhällsproblem och därför skulle straffet vara avskräckande

[190] 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.
[191] BrB 23:4.
[192] Holmqvist, Lena, Leijonhufvud, Madeleine, Träskman, Per Ole och Wennberg, Suzanne (red.), *Brottsbalken: en kommentar. Del 2, (13-24 kap.): brotten mot allmänheten och staten m.m.*, 7., [omarb.] studentutg., Norstedts juridik, Stockholm, 2013, BrB 24:5.
[193] Jareborg, Nils, *Påföljdsbestämningens struktur,* SvJT 1992 [s.258-275], s. 258 f.

för allmänheten.[194] HD har i ett andra fall medgett strafflättnad när en person dragits in ett händelseförlopp och endast kort hållit vakt och tagit emot ett fönster vid ett inbrott.[195] I detta fallet lade HD vikt vid att personen inte hade deltagit i hela händelseförloppet eller varit med och planerat brottet. HD beslutade i ett annat fall att inte ge någon strafflättnad trots att en person vid utförandet av själva brottet bara medverkat i mindre mån eftersom personen dels hade varit med i planeringen av brottet och dels deltagit under hela tiden brottet utfördes trots att det bara var i mindre mån.[196]

Strafflättnadsregeln borde i dagsläget kunna tillämpas om en tillhandahållare av Tor-noder skulle anses medverka till brott eftersom anonymitet och tillhandahållande av bandbredd i Tor-nätverket endast i liten utsträckning påverka fullbordan av huvudbrottet. Tillhandahållare av Tor-noder borde inte heller kunna anses vara delaktiga i planerandet av brott eftersom tillhandahållarna på förhand inte kan välja vilken trafik som går via deras noder. Tillhandahållarna bör inte heller anses vara med under hela händelseförloppet eftersom ingen enskild Tor-nod överför trafiken från användaren hela vägen till slutdestinationen såsom beskrivits i avsnitt 1.1.3.

8.6. Summering

Inledningsvis behöver det understrykas att redogörelsen ovan inte tar avstamp i något specificerat fall eller brott och att det därför inte med säkerhet går att fastslå att en domstol i ett enskilt fall skulle resonera i linje med redogörelsen. Tillhandahållande av Tor-noder erbjuder främst ett verktyg som försvårar identifieringen av användarna av nätverket, även om det också möjliggör att trafik överförs genom nätverket till det önskade slutmålet.

Eftersom tillhandahållare av Tor-noder inte har någon innehållsmässig korrespondens med användarna bör det anses vara uteslutet att tillhandahållande av Tor-noder genom psykisk påverkan skulle kunna få användare att begå brott endast genom att tillhandahålla Tor-noder. Ansvar för anstiftan till brott bör därför inte kunna åläggas tillhandahållare av Tor-noder endast på grund av tillhandahållandet.

Ansvar för medhjälp genom psykisk påverkan kräver likt anstiftan att det funnits någon form av innehållsmässig korrespondens mellan tillhandahållare av Tor-noder och användarna vilket det inte gör. Även om användare skulle bli mer benägna att utföra brott på grund av Tor måste

[194] TPB-domen s. 46-47.
[195] NJA 2006 s. 577.
[196] NJA 2009 s. 599.

det finnas ett psykiskt samband mellan tillhandahållarens främjande och användarens handlingar vilket inte kan uppnås endast genom tillhandahållandet av Tor-noder.

För att kunna hållas ansvarig för medhjälp genom fysisk påverkan krävs att tillhandahållandet av Tor-noder anses utgöra ett främjande av brott i lagens mening. Tillhandahållande av anonymitet bor inte kunna anses utgöra ett främjande eftersom anonymiteten i sig inte utgör ett främjande av huvudbrottet. Däremot skulle tillhandahållande av bandbredd objektivt sett kunna anses utgöra ett främjande av huvudbrottet eftersom tillhandahållarna möjliggör att trafiken överförs i nätverket och kan nå slutmålet.

Däremot har tillhandahållare av Tor-noder inte tillräcklig kännedom om den trafik som går genom deras noder för att kunna ha det uppsåt som krävs för att hållas straffrättsligt ansvariga för medhjälp till brott. Tor-nätverkets karaktär och hur användare väljer att utnyttja tjänsten utgör inte heller sådana indikationer på brottslig verksamhet som skulle innebära att tillhandahållare av Tor-noder ska anses ha kännedom om brott.

Därför bör tillhandahållande av Tor-noder i sig inte kunna anses utgöra straffbar medhjälp till brott som begås av användarna när Tor används.

Tillhandahållare av Tor-noder bör inte heller kunna anses bli ansvariga för oaktsam medverkan eftersom de saknar tillräcklig insikt i den trafik som går via deras noder och ska inte anses behöva göra något för att komma till den insikten eftersom det skulle innebära orimliga åtgärder från tillhandahållarnas håll.

Det bör här även noteras att det som huvudregel inte är tillåtet att övervaka eller avlyssna trafik eller ta del av andras meddelanden.

Skulle det anses som att tillhandahållare av Tor-noder främjar huvudbrott genom sitt tillhandahållande bör det finnas möjlighet att tillämpa den rättfärdigande omständigheten social adekvans eftersom syftet med Tor är legitimt och det av konstruktionen av Tor-nätverket inte finns något som indikerar att nätverket är uppbyggt i syfte att främja brottsliga aktiviteter.

Det bör även anses vara möjligt att tillämpa straffnedsättningsregeln i BrB 23 kap. 5 § i det fall att fler personer anses medverkat till huvudbrottet, eftersom tillhandahållare av Tor-noder bland annat inte genom tillhandahållandet medverkar under hela händelseförloppet.

Det ska därför konstateras att ansvar för medverkan till brott genom att tillhandahålla Tor-noder inte borde kunna åläggas tillhandahållare av Tor-noder enligt svensk lag.

9. Ansvarsfrihetsregeln i e-handelslagen

Utöver straffrättsliga regler finns det för tillhandahållare av vissa elektroniska tjänster även ett specifikt undantag från ansvar i e-handelslagen (”EHL”)[197]. Regeln innebär att tillhandahållare av tjänster som uteslutande består av överföring eller lagring av information för någon annans räkning endast åläggs straffrättsligt ansvar om tillhandahållaren haft uppsåt till det brott som innehållet i informationen avser.[198] För att kunna omfattas av ansvarsfrihet krävs att tillhandahållaren av Tor-noder är en tjänsteleverantör enligt EHL:s mening. Tidigare har tillhandahållare av sökmotorer, ISP:er och serverägare ansetts utgöra sådana tjänsteleverantörer.[199] Regeln är alltså tillämplig både på överförings- och lagringstjänster. Tor bör anses hänföra sig till överföring och inte till lagring, liksom exempelvis TPB.

Den som tillhandahåller tjänster som normalt utförs mot ersättning och som tillhandahålls på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare, tillhandahåller informationssamhällets tjänster.[200]

Tillhandahållande av Tor-noder bör anses ske på *distans* eftersom användaren och tillhandahållaren av Tor-noder inte närvarar fysiskt på samma plats när tjänsten levereras.[201] Tor tillhandahålls också via elektromagnetiska medel och tas emot med hjälp av utrustning för elektronisk behandling, varför det kan anses som att Tor tillhandahålls på *elektronisk väg*.[202]

För att en tjänst ska tillhandahållas på *individuell begäran* krävs viss interaktion mellan beställaren (användaren) och tillhandahållaren. Det krävs dock inte någon uttrycklig beställning i lagens mening utan syftet är att utesluta tjänster som tillhandahålls ett obegränsat antal mottagare samtidigt, exempelvis TV-tjänster.[203]

Eftersom Tor-nätverket endast är tillgängligt för de användare som har laddat ner mjukvaran och konfigurerat sin enhet bör det anses som att tillhandahållande av Tor-noder vänder sig till den begränsade kretsen av användare av Tor och att användarna genom att utnyttja Tor begär tjänsten. Tillhandahållande av Tor-noder kan därför anses utföras på individuell begäran.

Det återstående kriteriet *normalt utförs mot ersättning* behöver förklaras närmare.

---

[197] Lag om elektronisk handel och andra informationssamhällets tjänster (SFS 2002:562).
[198] EHL 19 §.
[199] Prop. 2001/02:150, s. 110.
[200] EHL 2 § 1 p.
[201] Prop 2001/02:150, s. 57.
[202] Prop. 2001/02:150, s. 57.
[203] Dir. 98/48/EG, Bilaga V.

Enligt förarbetena krävs det inte att tjänstemottagaren betalar direkt för tjänsten utan det räcker med att tjänsten i fråga normalt är av *ekonomisk betydelse*.[204] Typiskt sett hänför sig ”ekonomisk betydelse” till näringsverksamhet och innebär alla aktiviteter som har ett kommersiellt syfte.[205] Det sker inget utbyte av prestationer mellan tillhandahållare av Tor-noder och användare av Tor och Tor finansieras inte heller av reklamintäkter såsom TPB. Svea hovrätt ansåg precis som Stockholms tingsrätt att TPB tillhandahölls mot ersättning trots att användarna inte betalade någon avgift för tjänsten, eftersom hemsidan åtminstone delvis var reklamfinansierad.[206]

Frågan är alltså om tillhandahållande av tjänsten Tor genom tillhandahållande av Tor-noder kan anses vara av ekonomisk betydelse. Det ska inte läggas någon vikt vid att det i det aktuella fallet inte utgår någon ekonomisk ersättning för tjänsten eftersom även ideella organisationer och universitet har ansetts kunna tillhandahålla informationssamhällets tjänster trots att någon ekonomisk gottgörelse från användarna inte sker.[207]

En liknande tjänst skulle kunna vara virtuella privata nätverk (”VPN”)-tjänster, dels eftersom det likt Tor skapas en tunnel, ofta krypterad, som skydd för transporten av trafik mellan användaren av VPN-tjänsten och VPN-noden och dels eftersom det i vissa fall är VPN-nodens bandbredd som utnyttjas samt ip-adress som syns när trafiken går ut från tjänsten. En annan likhet är att det behövs någon som tillhandahåller VPN-noder vilket både privatpersoner och företag i dagsläget gör, flera företag gör det i dagsläget även mot betalning. Den största skillnaden mellan de som driver Tor-noder och de som driver VPN-noder är dock att de som driver VPN-noder har full kontroll över när deras noder förmedlar trafik samt att trafiken endast gör ett ”hopp” mellan användaren och slutdestinationen.

En annan jämförelse skulle kunna vara krypteringstjänster av meddelanden, men eftersom Tor innefattar kryptering av all form av trafik och inte bara meddelanden i sig är en sådan jämförelse missvisande. VPN-tjänster är därmed den mest näraliggande tjänsten som prövningen fortsatt kan utgå ifrån. VPN-tjänster nämns dock inte explicit som exempel på tjänster som normalt tillhandahålls mot ersättning i varken lagkommentaren[208] eller i förarbetena varför redogörelsen först måste ske av VPN-tjänster i förhållande till lagstiftningen.

[204] Notera att det är ett annat krav för EHL än det för LEK avsnitt 3.1.
[205] Prop. 2001/02:150, s. 56 f.
[206] Mål nr B 13301-06, Stockholms tingsrätt, 2009-04-17, s. 74.
[207] Prop. 2001/02:150, s. 57.
[208] Stålhandske, Jan, Kommentar till Lag (2002:562) om elektronisk handel och andra informationssamhällets tjänster, Karnov, 2015-04-01.

Det finns onekligen en betalningsvilja för VPN-tjänster hos användarna vilket innebär att tjänsten är av en sådan beskaffenhet att det finns möjlighet att ta betalt eller exempelvis finansiera tjänsten med reklam. Detta görs redan idag i viss omfattning. Det faktum att det tillhandahålls VPN-tjänster som liknar Tor mot betalning skulle alltså kunna innebära att tillhandahållande av Tor-noder har ekonomisk betydelse. Det går dock inte att dra ett likhetstecken mellan betalningsvilja och ekonomisk betydelse utan det är vad som är normalt för tillhandahållandet som styr. Slutsatsen bör dock i fråga om VPN-tjänster vara att tjänsten normalt utförs mot ersättning eftersom det de facto finns en omfattande mängd kommersiella tillhandahållare som tillhandahåller tjänsten mot ersättning.

Eftersom VPN-tjänster är mest närliggande Tor-nätverket gällande denna redogörelse bör slutsatsen trots att det råder oklarheter kunna anses vara att även Tor enligt kriterierna i EHL kan tillhandahållas mot ersättning. Ännu har dock någon domstol eller myndighet inte tagit ställning i frågan om VPN-tjänster bör omfattas av e-handelslagen varför denna fråga återstår att klargöras.

Det bör dock kunna antas att Tor är en sådan tjänst som är av ekonomisk betydelse och som normalt tillhandahålls mot ersättning. Alltså bör tillhandahållare av Tor-noder anses vara tillhandahållare av informationssamhällets tjänster i enlighet med EHL 2 §.

För att ansvarsfrihet ska kunna medges krävs enligt svensk rätt i nästa steg att tillhandahållaren saknar uppsåt till det brott som innehållet i informationen utgör.[209]

Gällande Tor-noder är det som beskrivits i avsnitt 8.3 mycket svårt för tillhandahållare av Tor-noder att få kännedom om vilken trafik som passerar genom tillhandahållarens noder. Det saknas som tidigare beskrivits (bland annat i 8.2.3) även kännedom om hur stor del av trafiken som går till sidor med otillåtet material eller hur många som använder sig av Tor-nätverket för att dölja sin identitet vid utförande av brott. Det är därför osannolikt att tillhandahållare av Tor-noder skulle ha eller kunna uppnå den kännedom om innehållet i trafiken som krävs för att ha uppsåt i lagens mening.

EU-domstolen har uttalat sig i frågan om när en tjänsteleverantör ska anses sakna kännedom om innehållet och därmed även uppsåt till ett brott.

Det är främst i två avgöranden som EU-domstolen har klargjort sin ståndpunkt vilket är i Google-domen[210] och i L'Oreál-domen[211]. I dessa domar framhåller EU-domstolen att

[209] EHL 19 §.

tjänstleverantörens passivitet och uteblivna kännedom om informationen ska tillmätas stor betydelse vid bedömningen av ansvarsfrihet. De kriterier som EU-domstolen uttolkat från direktivet är att tjänsteleverantörens funktion ska vara av rent teknisk, automatisk natur och behandling av uppgifter från kunderna ska ske på ett neutralt sätt vid tillhandahållande av tjänsterna för att ansvarsfrihet ska kunna tillämpas.

Tillhandahållande av Tor-noder sker utan att tillhandahållarna aktivt behöver befatta sig med den information som förmedlas. Efter att tillhandahållaren konfigurerat sin enhet består tillhandahållarens aktivitet endast av att betala för bandbredd och el eller i vissa fall hyra för servrar, men själva tjänsten kräver ingen aktivitet från tillhandahållaren. Tillhandahållandet av Tor-noder sker även automatiskt genom att algoritmer som tillhandahållaren inte kan påverka dirigerar trafiken genom noderna utan att tillhandahållaren behöver godkänna eller på annat sätt välja vilken användare eller vilken information som ska överföras.

Tillhandahållare av Tor-noder saknar därigenom även kännedom om den information som överförs via de tillhandahållna Tor-noderna. Detta torde innebära att ansvarsfrihetsregeln skulle kunna tillämpas på tillhandahållande av Tor-noder även om den information som överförs omfattar brottsligt material.

Mot bakgrund av denna slutsats aktualiseras dock återigen frågan om tillhandahållande av Tor-noder kan anses vara en tjänst eller endast en del av en tjänst. Eftersom det oftast är fler än en tillhandahållare av Tor-noder som tillhandahåller hela kretsen av Tor-noder för klientens trafik är frågan om var och en av tillhandahållarna i ledet kan anses tillhandahålla informationssamhällets tjänster för driften av sina Tor-noder.

Enligt e-handelsdirektivet[212] ges bland annat ISP:er och serverägare som exempel på av vad som inryms i definitionen. Det som är gemensamt för samtliga exempel är att det finns en enhet som är tjänsteleverantör. Det är därför oklart om tillhandahållare av Tor-noder kan anses utgöra en tjänsteleverantör i lagens mening över huvud taget. Denna fråga är något som lagstiftaren eller domstolarna behöver klargöra innan ett säkert svar på frågan kan ges.

[210] Mål C-236/08, Google France SARL, Google Inc v. Louis Vuitton Malletier SA.
[211] Mål C-324/09, L'Oréal SA m.fl v. eBay International AG m.fl.
[212] Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden ("Direktiv om elektronisk handel").

9.1 Summering

Ansvarsfrihetsregeln i EHL bör kunna tillämpas om tillhandahållare av Tor-noder anses medverka till annans brottslighet genom tillhandahållandet. Anledningen är dels att tillhandahållare av Tor-noder bör kunna anses utgöra tillhandahållare av informationssamhällets tjänster och dels att de svårligen kan få insyn i de meddelanden eller trafik som användare av Tor-noder skickar via deras noder.

Eftersom tillhandahållarna svårligen kan få den insyn som krävs kan de inte heller ha uppsåt till innehållet i det som överförs och därmed bör tillhandahållare av Tor-noder enligt EHL kunna få ansvarsfrihet för tillhandahållande av Tor-noder även om användare utnyttjat deras noder för utförande av brott.

10. Straffrättsligt ansvar för tillhandahållande av Tor-noder i juridiska personer

Enligt straffrätten är det bara fysiska personer som kan hållas ansvariga för brott, alltså inte juridiska personer såsom aktiebolag, föreningar och liknande. Ett brott som sådant kan ändå begås inom en juridisk persons verksamhet, men då är det fysiska personer som hålls ansvariga för brotten enligt allmänna straffrättsliga principer.

En anledning till att det bara är fysiska personer som kan hållas ansvariga för brott är skuldprincipen som berörs i 6.2.3 och innebär att det krävs uppsåt eller i vissa fall oaktsamhet för att kunna hållas straffrättsligt ansvarig och det är bara fysiska personer som har förmåga till uppsåt eller oaktsamhet.[213]

Om ett företag eller en förening vill tillhandahålla Tor-noder är det därför viktigt att ta reda på vilket ansvar som kan uppkomma och vem som kan bli ansvarig inom organisationen.

Som ovan konstaterats bör det påminnas om att tillhandahållare av Tor-noder i dagsläget inte borde kunna hållas straffrättsligt ansvariga för tillhandahållande av Tor-noder varken som gärningspersoner eller som medverkanspersoner.

10.1. Ansvar för juridiska personer

I vissa fall kan juridiska personer ”straffas” genom *företagsbot*[214] vilket utgör en så kallad *särskild rättsverkan av brott* och består av en ekonomisk sanktion på maximalt 10 miljoner kronor. Företagsbot är alltså inte en brottspåföljd som ersätter det individuella straffansvaret.[215]

Kraven för att bli ålagd företagsbot är att ett brott har begåtts i näringsverksamhet eller att det har klar anknytning till näringsverksamheten och att brottet har ett strängare straff än penningböter. Det krävs också antingen att näringsidkaren själv inte gjort vad den borde för att förebygga brottet eller att brottet har begåtts av en person i ledande ställning som haft rätt att företräda eller fatta beslut på näringsidkarens vägnar eller att en person haft särskilt ansvar för tillsyn eller kontroll i verksamheten.

[213] Asp, Ulväng och Jareborg, s. 65 f.
[214] BrB 36:7.
[215] Proposition 2005/06:59, *Företagsbot*, s. 14.

Näringsidkare betyder enligt lagen både fysiska och juridiska personer som yrkesmässigt bedriver verksamhet av ekonomiskt slag, oavsett om verksamheten är inriktad på vinst eller inte.[216]

Bestämmelsen om företagsbot tar framförallt sikte på så kallad näringsreglerande lagstiftning såsom lagar inom miljö, arbetsmiljö, och andra brott mot krav på tillstånd vilket även framgår av praxis.[217] Ett av argumenten för att sanktionera näringsidkare för dessa brott är att uppkomsten av den typen av brott ofta är sammankopplade med företagens organisation och struktur och att incitamenten för att bedriva en välorganiserad verksamhet därför skulle öka.[218] Detta innebär samtidigt att bestämmelsen inte uteslutande omfattar brott mot näringsrelaterad lagstiftning.

Ett brott skall alltså anses begånget i näringsverksamhet om det ingår som ett led i en näringsidkares verksamhet. Det skall typiskt sett ha en klar anknytning till den verksamhet som bedrivs av personen, antingen i sin egenskap av näringsidkare, företrädare för eller anställd hos den som bedriver näring.[219]

I en tingsrättsdom ansågs till exempel takläggning och rörmokeri inte ligga alltför långt från varandra hantverksmässigt och det ansågs därför att det takläggningsarbete som gjorts hade en sådan klar anknytning till rörmokeri att det ansågs vara utfört i näringsverksamheten hos den som bedrivit rörmokeriverksamhet.[220]

I en dom från HD dömdes en chefredaktör för anstiftan, en nyhetschef för medhjälp och en journalist för vapenbrott.[221] Målet handlade om en journalist som fick i uppdrag att skriva en artikel om hur lätt det var att köpa vapen i Malmö och skulle för att visa detta alltså köpa ett vapen för att sedan direkt överlämna det till polisen. I domen berörs aldrig frågan om företagsbot eller eventuellt ansvar för andra än de som haft kännedom om vad som skulle göras och varit delaktiga i planering och händelseförlopp genom att ha kommunicerat med varandra. Varför frågan om företagsbot inte togs upp är inte känt, men detta mål hade varit ett

[216] Prop. 2005/06, s. 20.
[217] MÖD 2001:22, MÖD 2001:23, MÖD 2001:24, NJA 1991 s. 783, NJA 1999 s. 87, NJA 2001 s. 579, NJA 2007 s. 369, NJA 2012 s. 826, NJA 2014 s. 139, RH 1999:84, RH 2009:30, RH 2009:41, RH 2011:54, RH 2013:13 och RH 2013:7.
[218] Prop. 2005/06, s. 23.
[219] Prop. 2005/06, s. 20.
[220] Mål nr B 4754-11, Skaraborgs tingsrätt, 2012-03-27, det kan noteras att det finns mycket knapphändigt med rättsfall rörande förtagsbot som gäller brott mot näringsreglerande verksamhet såsom arbetsmiljö, tillståndspliktig verksamhet och liknande.
[221] Mål nr B 1471-13, Högsta domstolen, 2015-03-04, http://www.hogstadomstolen.se/Domstolar/hogstadomstolen/Avgoranden/2015/2015-03-04%20B%201471-13%20dom%20skiljaktig%20mening.pdf.

bra tillfälle att pröva hur långt från den dagliga verksamheten ett brott kan ligga för att fortfarande anses ha anknytning till verksamheten och leda till företagsbot för den juridiska personen.

Tillhandahållande av Tor-noder skulle i vissa fall kunna anses ha sådan anknytning till näringsverksamheten att ansvar för tillhandahållande skulle kunna falla på den juridiska personen. De tydligaste exemplen borde vara tillhandahållare av VPN-tjänster och ISP:er eftersom båda dessa näringsverksamheter innebär tillhandahållande av bandbredd för överföring av trafik. Det är dock mer oklart om tillhandahållande av Tor-noder av en tidningsredaktion eller en förening som arbetar med yttrandefrihetsfrågor skulle anses ha en klar koppling till näringsverksamheten.

Mot bakgrund av redogörelsen i avsnitt 7 och 8 är det dock tveksamt om ansvar för tillhandahållande av Tor-noder skulle kunna uppkomma över huvud taget.

10.2. Ansvar för fysiska personer inom en juridisk person

Även fysiska personer inom en juridisk person kan ådra sig ansvar för sin egen och andras brott.

En person som på order av någon med ledande ställning konfigurerar en enhet till att bli en Tor-nod kan inte enbart för detta agerande hållas straffrättsligt ansvarig eftersom själva konfigurationen av en enhet över huvud taget inte utgör något brott.

Om en juridisk person tillhandahåller Tor-noder behöver den fysiska tillhandahållaren på något sätt dock identifieras. En rimlig slutsats borde vara att det är den som har rätt att uppdra åt någon eller att själv konfigurera enheten som utgör den fysiska tillhandahållaren. Det borde även vara en person som har ett ansvar att se till att noden förses med el och internetanslutning. På en redaktion skulle det kunna vara redaktionschefen som är ansvarig, i en förening en generalsekreterare och i ett aktiebolag VD:n eller liknande. Att en styrelse skulle åläggas ansvar för tillhandahållande av Tor-noder borde inte vara en rimlig slutsats eftersom de i de flesta fall står för långt ifrån den dagliga verksamheten och saknar den praktiska möjligheten till kontroll över Tor-noderna.

Det ansvar som skulle kunna åläggas den ansvariga i en organisation är detsamma som redogjorts för i avsnitt 7 och 8. Baserat på redogörelserna i dessa avsnitt bör dock tillhandahållare av Tor-noder inom juridiska personer svårligen kunna åläggas straffrättsligt ansvar för tillhandahållandet.

10.3. Summering

Juridiska personer kan inte hållas straffrättsligt ansvariga för brott såsom fysiska personer. Däremot finns det möjlighet att påföra juridiska personer företagsbot som utgör en särskild rättverkan av brott i det fall ett brott har blivit begånget som ett led i näringsverksamheten eller om brottet haft klar anknytning till den juridiska personens verksamhet.

Beroende på den juridiska personens verksamhet kan tillhandhållande av Tor-noder anses ha en så klar anknytning till näringsverksamheten att den juridiska personsonen skulle kunna påföras företagsbot i de fall användare av de tillhandahållna Tor-noderna begår brott.

Straffrättsligt ansvar för någon inom organisationen borde kunna åläggas den person som har rätt att uppdra åt någon eller att själv konfigurera noderna och ansvarar för driften av Tor-noderna. Ansvarsbedömningen av denna person ska göras i enligt med avsnitt 7 och 8.

Mot bakgrund av att det tidigare i denna rapport (se avsnitt 7 och 8) konstaterats att tillhandahållare av Tor-noder svårligen bör kunna hållas straffrättsligt ansvariga enbart på grund av tillhandahållandet av Tor-noder, är risken för både företagsbot och personligt ansvar för någon i organisationen bedömt relativt låg.

Del 3 Tvångsmedel och internationella erfarenheter

11. Tvångsmedel

Om rättsvårdande myndigheter trots slutsatsen i avsnitt 7 och 8 skulle anse att en tillhandahållare av Tor-noder kan hållas straffrättsligt ansvariga för tillhandahållande av Tor-noder är det av stort intresse att utröna vilka tvångsmedel som skulle kunna aktualiseras. Främst är detta en fråga för de fysiska och juridiska personer som har känslig information, exempelvis källor i journalistiskt arbete eller medlemsregister, sparade hos sig elektroniskt.

Även om tillhandahållare av Tor-noder inte skulle kunna åläggas straffrättsligt ansvar för tillhandahållandet finns det möjlighet för rättsvårdande myndigheter att använda tvångsmedel mot tillhandahållarna. Inte för att de har någon medveten koppling till det utförda brottet utan för att rättsvårdande myndigheter skulle kunna anse att tillhandahållare har sådan information som är av värde för brottsutredningen.

Redogörelsen i denna del tar alltså sikte på tvångsmedel i brottmål och inte i tvistemål (civilprocesser). Regler om tvångsmedel i tvistemål kommer därför inte att beröras. De tvångsmedel som kommer att beröras är beslag, husrannsakan och vissa hemliga tvångsmedel.[222]

Som beskrivits i avsnitt 1.1 kan Tor-noder drivas på alla typer av lagringsmedia. Detta innebär att det exempelvis på en hemmadator går att driva en Tor-nod. Om Tor-noder drivs via datorer som också används för annat bruk återfinns all data som är sparad på lagringsmediet samt en krypteringsnyckel för Tor-noden på den konfigurerade enheten.

Krypteringsnyckeln som sparas på varje Tor-nod kallas för *identity key* (”IK”) eller *master identity key* (”MIK”) beroende på vilken version av Tor som används. Krypteringsnyckeln är Tor-nodens identitet. Den som har tillgång till IK eller MIK kan utge sig för att vara Tor-noden, det vill säga starta en Tor-nod med samma identitet som den ursprungliga Tor-noden. Tillgången till IK eller MIK ger ingen möjlighet att få fram någon information om historiskt data eller annat, alltså går det inte att få fram någon information om den trafik som redan passerat genom Tor-noden med hjälp av IK eller MIK.

[222] RB kapitel 27 och 28.

Nyligen[223] har det blivit möjligt att lagra MIK på en separat enhet. Detta innebär att MIK kan sparas på en annan enhet än i Tor-noden som tillhandahålls.[224] Detta kräver en del extrajobb för tillhandahållarna och det finns idag ingen statistik på hur många som har valt att utnyttja denna möjlighet. Funktionen innebär dock att det nu finns en möjlighet att tillhandahålla ”helt tomma” Tor-noder.

11.1. Beslag

Beslag[225] innebär att rättsvårdande myndigheter har rätt att omhänderta föremål i tre olika fall: 1) *utredningsbeslag* som syftar till att underlätta utredning av brott, 2) *förverkandebeslag* som syftar till att det beslagtagna i framtiden ska förverkas och 3) *återställandebeslag* som syftar till att lämna tillbaka ett föremål till någon som har blivit av med det genom brott.[226]

Beslag av Tor-noder skulle rimligvist bara bli aktuellt om det utgör ett utredningsbeslag. Därför ska förutsättningar för utredningsbeslag beröras här. Beslag kan beslutas för alla typer av brott och vid vilken tidpunkt som helst under en förundersökning eller efter det att åtal har väckts. Beslutet kan till och med fattas så tidigt under förundersökningen att det ännu inte finns någon misstänkt gärningsperson som är identifierad.[227] Utredningsbeslag syftar de facto ofta till att försöka identifiera den misstänkta gärningspersonen.[228]

Det krävs inte heller någon särskild allvarlighetsgrad på brottet generellt, men det krävs att det finns misstanke om ett konkret brott och att det finns konkreta omständigheter som med viss styrka tyder på att föremålet som ska beslagtas kommer att underlätta utredningen av brott.[229]

Beviskravet för att kunna beslagta ett föremål är att det *skäligen kan antas* att föremålet har betydelse för utredningen av ett brott. Det är ett relativt lågt ställt krav på bevis men inte det lägsta och kan jämställas med misstankegraden ”skäligen misstänkt”.[230]

Beslut om beslag får om det inte sker vid en husrannsakan, gripande av misstänkt eller liknande göras av en undersökningsledare eller åklagare.[231] Eftersom Tor-noder normalt torde

[223] Tor version 0.2.7.2-alpha släppt den 2015-07-27.
[224] I korthet fungerar detta så att en krypteringsnyckel kan signeras med en annan krypteringsnyckel och på så vis behålls MIK:en på ett säkrare ställe medan en "medium term key" kopieras till en internetansluten enhet då och då. Denna "medium term key" har typiskt en kortare livslängd på cirka sex månader.
[225] RB 27:1.
[226] Lindberg, Gunnel, *Rättegångsbalk (1942:740) 27 kap. 1 §*, Lexino 2015-07-01, 2.1.
[227] Lindberg, Lexino, 2.1.
[228] Lindberg, Lexino, 2.4.
[229] SOU 1995:47, *Tvångsmedel enligt 27 och 28 kap. RB samt polislagen*, Slutbetänkande av Polisrättsutredningen, s. 357.
[230] Nordh, Roberth, *Tvångsmedel: kvarstad, häktning, beslag, husrannsakan m.m.*, Iustus, Uppsala, 2007, s. 92 samt Lindberg, Lexino, 2.3.

tillhandahålls från någon form av byggnad eller slutet förvaringsställe är utgångspunkten för den fortsatta redogörelsen att det krävs ett beslut om husrannsakan för att få tillgång till Tor-noder. En närmare redogörelse för husrannsakan framgår av avsnitt 11.2.

Beslag får ske hos den som har föremålet, vilket innebär att beslag får göras också hos en utomstående person och inte bara är hos målsägande eller den misstänkta gärningspersonen.[232] Tor-noder skulle alltså eventuellt kunna beslagtas även om tillhandahållaren saknar kännedom om att ett brott begåtts. Men för att beslag ska kunna ske krävs att flera förutsättningar föreligger.

Det finns begränsningar i vilka föremål som kan beslagtas.[233] Beslagsförbudet innebär bland annat att det genom beslaget inte ska gå att inhämta mer information från vissa yrkesutövare än vad som kan delges vid vittnesförhör med dessa.[234] Exempel på yrkesutövare är journalister[235], advokater[236] och präster[237]. Förbudet omfattar alltså inte all information som dessa yrkesutövare besitter, utan endast den som omfattas av den yrkesmässiga tystnadsplikten. För journalister är sådan information exempelvis uppgifter om källor.

Frågan om beslag av lagringsenheter hos en tidningsredaktion avgjordes nyligen av HD i den så kallade ”Aftonblandet-domen”.[238] HD slår i domen fast att beslagsförbudet är absolut och inte kan genombrytas efter en intresseavvägning eller proportionalitetsbedömning.[239] En av frågorna som HD behandlade var dock hur beslagsförbudet ska tillämpas vid beslag av filer på lagringsenheter där sådan information som inte ska beslagtas, så kallad sidoinformation, även finns och är skyddad mot beslag. Bland annat förde HD ett resonemang om att det i vissa fall ska kunna göras en proportionalitetsbedömning.

För att en liknande fråga som i Aftonblandet-domen ska aktualiseras på grund av tillhandahållande av Tor-noder behöver tillhandahållaren utöver att konfigurera enheten till Tor-nod även spara skyddad information på enheten.

---

[231] RB 27:4 st. 2.
[232] Lindberg, Lexino, 2.8.
[233] RB 27:2.
[234] RB 36:5.
[235] RB 36:5 st. 6, ” Den som har tystnadsplikt enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen får höras som vittne om förhållanden som tystnadsplikten avser endast i den mån det föreskrivs i nämnda paragrafer.”
[236] RB 36:5 st. 2.
[237] RB 36:5 st. 5.
[238] NJA 2015 s. 631.
[239] NJA 2015 s. 631, p. 20.

En annan förutsättning för att en liknande fråga ska uppkomma är att information som sparas på enheten till följd av tillhandahållande av Tor-noder tillåter att ett beslag görs. Fråga om beslag av Tor-noder ska därför först utredas under förutsättning att det saknas annan information än IK eller MIK på enheten, varför frågan blir om denna information kan ge skäl att beslagta enheter.

Vid beslut om beslag krävs enligt lagtexten att skälen väger upp det intrång ett beslag innebär.[240] Det krävs alltså att åtgärden är *proportionerlig* i förhållande till det syfte som föremålet ska beslagtas för. Detta innebär att om samma information kan kommas åt genom en minde ingripande åtgärd än beslag ska denna användas. Proportionalitetsbedömningen görs mellan omständigheter som art, styrka, räckvidd, varaktighet och målet med ingripandet.[241]

Det krävs alltså att informationen på Tor-noderna skäligen kan antas ha betydelse för utredningen av ett brott för att de ska kunna beslagtas.

Såsom beskrivits tidigare i detta avsnitt sparas ingen information på Tor-noderna utom en krypteringsnyckel som anger nodens identitet. Denna information kan inte användas för några andra ändamål än att tillhandahålla en Tor-nod med den samma identiteten.

Det kan mot bakgrund av det ovanstående svårligen anses som att information på enheter som endast utgör Tor-noder skäligen kan antas ha betydelse för utredning av brott. Bedömningen bör därför vara att ingreppet bör anses för omfattande i förhållande till den information som kan inhämtas genom beslag. Beslag av Tor-noder torde därför utgöra en oproportionerlig handling eftersom målet med beslaget inte kan uppnås genom handlingen.

Av detta följer vidare att frågan om hur skyddad sidoinformation ska behandlas vid beslag inte bör aktualiseras vid tillhandahållande av Tor-noder även om lagringsenheter som innehåller skyddad information också konfigureras till Tor-noder. Detta eftersom den information som sparas på enheten till följd av konfigurationen inte utgör sådan information som skäligen kan antas ha betydelse för utredningen av brott bör den därmed inte heller anses väga upp det intrång som ett beslag innebär.

Skulle enheten även användas för andra ändamål kan det finnas anledning att det på den grunden beslagta enheten, men detta har då inget samband med tillhandahållande av Tor-noder.

[240] RB 27:1 st. 3.
[241] Lindberg, Lexino, 2.9.

Det föreligger dock en viss risk för att rättsvårdande myndigheter saknar kännedom om hur Tor-noder fungerar och därför kan tro eller misstänka att det lagras mer omfattande information på enheten. Med ledning av Aftonbladet-domen kan dock skyddad information undanhållas från beslag genom att inför domstol med viss konkretion visa att det finns information på enheten som omfattas av beslagsförbudet.[242]

Det är sedan endast domstol, undersökningsledare och åklagare som har rätt att ta del av innehållet på enheterna.[243] Det föreligger olika uppfattningar om det också behövs tillstånd för husrannsakan för att gå igenom informationen på en hårddisk och om hur de digitala kopiorna ska behandlas vilket kommer att redogöras för i avsnitt 11.2.[244]

Eftersom beslag i vissa fall kan vara oproportionerligt har det ibland föreslagits att innehållet på en hårddisk kan kopieras istället för att hela hårddisken ska beslagtas.[245] En teknik för detta är så kallad spegelkopiering och innebär att allt som finns på hårddisken kopieras, även det som raderats med ännu inte har skrivits över på enheten kopieras.[246]

Det finns idag ingen reglering av hur kopior av föremål som tagits i beslag ska hanteras.[247] Detta innebär att även om beslag har hävts kan polis och åklagare behålla kopior av beslagen vilket ökar risken för att information sprids inom myndigheterna.[248] Även här råder det tveksamheter kring om det krävs tillstånd för husrannsakan för spegling och kopiering. För närvarande pågår dock en utredning angående hur dessa frågor ska hanteras varför svar förhoppningsvis kommer att ges inom en relativt nära framtid.[249]

Motbakgrund av redogörelsen i detta avsnitt bör beslag av Tor-noder inte anses vara proportionerligt då informationen som genereras och sparas till följd av tillhandahållande av Tor-noder inte skäligen kan antas ha betydelse för utredning av brott.

11.2. Husrannsakan

Husrannsakan innebär att rättsvårdande myndigheter har tillstånd att gå in i hus, rum och slutet förvaringsställe för att leta efter föremål som ska beslagtas för att få reda på

[242] NJA 2015 s. 631, p. 31 samt p. 36.
[243] RB 27:12, jmf RB 28:8 angående husrannsakan.
[244] Lindberg, Gunnel, *Straffprocessuella tvångsmedel: när och hur får de användas?*, 3., [rev.] uppl., Karnov Group, Stockholm, 2012, s. 584 och 605, hänvisar i sin tur till lagförarbeten som ännu inte lett till någon lagstiftning om frågan.
[245] Nordh, s. 93.
[246] Lindberg, *Straffprocessuella tvångsmedel*, s. 445,
[247] Nordh, s. 93.
[248] Lindberg, Lexino, 3.3.
[249] Kommittédirektiv 2016:20, *Moderna regler om beslag och husrannsakan*, s. 9 f.

omständigheter som kan vara av betydelse för en brottsutredning eller för att hitta byte från brottslig verksamhet som ska förverkas.[250] Hus enligt lagtexten innebär alla former av byggnader medan rum innebär samtliga utrymmen i en byggnad exempelvis kontorslokaler och lagerlokaler.[251] I denna rapport kommer redogörelsen behandla husrannsakan i syfte att verkställa ett beslag. Husrannsakan kan tillskillnad mot beslag som behandlats i avsnitt 11.1 inte användas i brottsförebyggande syfte.[252]

Husrannsakan får beslutas av utredningsledare, åklagare och av domstol,[253] men om det är bråttom att verkställa husrannsakan får beslutet även fattas av polis.[254] I praktiken är det sällan domstolen fattar beslut om husrannsakan men det sker oftast när husrannsakan ska göras hos advokatkontor och tidningsredaktioner främst på grund av beslagsförbudet som behandlats i avsnitt 11.1.[255]

Beviskravet för att få tillstånd till husrannsakan är det samma som för att inleda en förundersökning, alltså att det ska finnas anledning att tro att ett brott har begåtts.[256] Det krävs konkreta omständigheter för att en sådan anledning ska uppstå. Det krävs också att fängelse finns i straffskalan för det brott som utreds, men det krävs inte att det i det enskilda fallet kommer att utdömas ett fängelsestraff för gärningen.

För att kunna göra husrannsakan hos annan än den som är skäligen misstänkt krävs att den misstänkta har begått brottet hos denna andra person, att den misstänkta har gripits hos denna eller om det finns synnerlig anledning att det kommer att påträffas föremål som kan tas i beslag eller förvar eller att annan utredning om brottet eller förverkande av utbyte av brottslig verksamhet kan fås genom husrannsakan.[257] För husrannsakan hos någon som inte är misstänkt krävs i det sista fallet att det tydligt går att visa att det finns skäl att förvänta sig att påträffa föremålet eller få andra uppgifter om brottet för att tillstånd ska beviljas. Detta understryks av formuleringen ”synnerlig anledning” som ställer krav på att det finns faktiska omständigheter i det enskilda fallet som pekar på detta.[258] Vid husrannsakan ska det även

[250] RB 28:1.
[251] Lindberg, Lexino, 1163) samt Nordh, s. 110.
[252] Nordh, s. 109.
[253] RB 28:4.
[254] RB 28:5.
[255] Nordh, 113 f.
[256] RB 23:1.
[257] RB 28:1 st. 2.
[258] Lindberg, Lexino, 1169) samt Nordh, s. 111.

närvara ett trovärdigt vittne som ordnats av den som utför husrannsakan, detta är inget absolut krav utan det ska ordnas så långt det är möjligt.[259]

Som beskrivits i 11.1 krävs det eventuellt tillstånd för husrannsakan för att få tillgång till Tor-noderna över huvud taget eftersom de sannolikt är placerade i en byggnad eller liknande. Såsom i samma avsnitt beskrivits är det fortfarande oklart om det också behövs tillstånd för husrannsakan för att kunna ta del av informationen på en hårddisk, men det står klart att det endast är domstol, utredningsledare och åklagare som har rätt att ta del av informationen som inhämtats genom husrannsakan.[260]

Det pågår förnärvarande en utredning i syfte att bland annat se över om det skulle vara möjligt att göra husrannsakan i en dator, ett datorsystem eller annan liknande teknisk utrustning via ett elektroniskt kommunikationsnät, alltså på distans.[261] Dessa frågor har tidigare utretts och förslag på att detta ska vara möjligt har lämnats utan att det lett till lagstiftning.[262]

Liksom vid samtliga tvångsmedel krävs det att husrannsakan är en proportionerlig handling i förhållande till målet med husrannsakan.[263] En liknande proportionalitetsbedömning som i 11.1 tillämpas även vid husrannsakan.

Som framgår av redogörelsen i 11.1 är den information som finns på Tor-noderna inte av sådant slag att enheterna bör kunna tas i beslag. Detta innebär därför att ett tillstånd för husrannsakan endast grundat på tillhandahållande av Tor-noder inte bör anses vara proportionerligt.

I Aftonbladet-domen som berörts i avsnitt 11.1 understryks även beslagsförbudet vid husrannsakan hos tidningsredaktioner:

> ”Regelverket innebär alltså att husrannsakan för att genom beslag åtkomma viss information som finns på en elektronisk informationsbärare hos en tidningsredaktion i allmänhet lär vara utesluten. Endast om det i det enskilda fallet är möjligt att mycket entydigt och snävt begränsa en genomsökning av

[259] RB 28:7.
[260] Jfr RB 28:8 som hänvisar till RB 27:12 angående beslag.
[261] Kommittédirektiv 2016:20, s. 4 f.
[262] Ds 2005:6, *Brott och brottsutredning i IT-miljö. Europarådets konvention om IT-relaterad brottslighet med tilläggsprotokoll*.
[263] RB 28:3 a.

> informationsbäraren, och därmed minimera risken för att skyddad information röjs, kan en sådan rannsakning vara förenlig med proportionalitetsregeln."[264]

Det kan därför inte anses vara tillåtet att få tillstånd för husrannsakan för att beslagta Tor-noder från en tillhandahållare som även behandlar skyddad information på enheten.

Husrannsakan för beslag av Tor-noder bör även generellt anses vara oproportionerligt mot bakgrund av att den information som genom husrannsakan kan inhämtas inte kan anses ha sådan betydelse för brottsutredning som krävs eftersom IK och MIK endast ger information om Tor-nodens identitet.

11.3 Hemliga tvångsmedel

Det finns flera former av hemliga tvångsmedel bland annat: 1) hemlig avlyssning av elektronisk kommunikation,[265] 2) hemlig övervakning av elektronisk kommunikation och,[266] 3) hemlig kameraövervakning[267]. I denna rapport ska endast hemlig avlyssning och övervakning av elektronisk kommunikation beröras eftersom tillhandahållande av Tor-noder involverar elektronisk kommunikation.

Hemliga tvångsmedel används vid förundersökningar för att utreda brott och kräver att det finns någon som är skäligen misstänkt.[268] För att få tillstånd till hemlig avlyssning och övervakning krävs att en domstol beslutar om detta på ansökan av åklagare.[269] Om en fördröjning av påbörjad avlyssning eller övervakning skulle ha väsentlig betydelse för utredning av brott får åklagare besluta om att inleda dessa åtgärder men måste direkt ansöka om ett tillstånd från domstol.[270]

Det finns förbud mot avlyssning och övervakning av elektronisk kommunikation i både LEK[271] och i BrB[272]. De aktuella tvångsmedlen innebär alltså ett avsteg från huvudregeln.

Hemlig avlyssning och övervakning tar sikte på att i hemlighet genom ett tekniskt hjälpmedel få tillgång till meddelanden som skickas eller har skickats via ett elektroniskt kommunikationsnät till eller från ett telefonnummer eller annan adress. Ett meddelande i

[264] NJA 2015 s. 631, p. 39.
[265] RB 27:18.
[266] RB 27:19 och 3.
[267] RB 27:20 a.
[268] Enligt RB 27:20, se Nordh, s. 102.
[269] RB 27:21.
[270] RB 27:21 a.
[271] LEK 6:17.
[272] BrB 4:8-9 c.

lagtextens mening är samtliga meddelanden innehållande ljud, text, bild, data eller information i övrigt som förmedlas med hjälp av radio, ljus eller elektromagnetiska svängningar som utnyttjar särskild anordnad ledare.[273] E-post är ett exempel på meddelande som omfattas av lagtextens begrepp.

Bestämmelserna om avlyssning och övervakning av elektronisk kommunikation knyter även an till reglerna i LEK[274] om att det är tillhandahållare av allmänna kommunikationsnät samt kommunikationstjänster av vissa slag som ska bereda möjlighet att verkställa hemlig avlyssning eller övervakning. Det är alltså endast de som omfattas av LEK som har en skyldighet att låta rättsvårdande myndigheter avlyssna eller övervaka den trafik som överförs genom deras tjänster och nät. Aktörer som utan beslut möjliggör eller själva avlyssnar eller övervakar trafik i allmänna elektroniska kommunikationsnät riskerar att begå en otillåten eller brottslig handling enligt LEK[275] eller BrB[276].

Baserat på redogörelsen i Del 1 i denna rapport är tillhandahållare av Tor-noder inte är skyldiga att möjliggöra avlyssning eller övervakning av de tillhandahållna Tor-noderna, utan detta ansvar ligger på ISP:er och andra operatörer. Detta betyder dock att de meddelanden som går via Tor-nätverket, om förutsättningar finnas (vilket är högst osannolikt baserat på de krav som ställs i lagen) kan avlyssnas eller övervakas genom användarnas och tillhandahållarnas ISP:er, men tillgång kan endast fås till begränsad information på grund av konstruktionen av Tor-nätverket såsom beskrivits i avsnitt 1.1.3.

Frågan som uppkommer baserat på detta är alltså vilken risk det finns för att meddelanden till och från användarna av Tor avlyssnas eller övervakas och inte en fråga om legala risker för dem som tillhandahåller Tor-noder. Denna fråga ligger därför utanför syftet med denna rapport och kommer inte att beröras vidare.

11.3.1 Utredning om hemlig dataavläsning

Det bör här noteras att det pågår en utredning om att tillåta hemlig dataavläsning.[277] Definitionen av hemlig dataavläsning är inte fastslagen men utredningen kommer enligt kommittédirektivet att basera sin analys på följande definition av begreppet:

[273] Proposition 2011/12:55, *De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation*, s. 58.
[274] LEK 6:19.
[275] LEK 6:17.
[276] BrB 4:8-9 c.
[277] Kommittédirektiv 2016:36, *Hemlig dataavläsning*.

> ”[…] som en metod för de brottsbekämpande myndigheterna att med någon form av tekniskt hjälpmedel i hemlighet bereda sig tillgång till en dator eller annan teknisk utrustning som används för kommunikation och därigenom få besked om hur utrustningen används i realtid och vilken information som finns i den. Detta kan t.ex. ske genom att en hård- eller mjukvara placeras, antingen fysiskt eller elektroniskt, via en eller flera trojaner, i en användares tekniska utrustning.”[278]

En av anledningarna till att utredningen tillsatts är att de hemliga tvångsmedel som idag används inte ger det resultat som önskas bland annat på grund av:

> ”[…] tekniska svårigheter med att avlyssna internetbaserad kommunikation inom ramen för ett tillstånd till hemlig avlyssning. Det beror framför allt på att enskilda personer enkelt kan köpa anonymiseringstjänster som skyddar deras identitet, ip-adress, på nätet så att kommunikationen blir helt anonym. Teknikutvecklingen har också medfört att det inte längre är självklart att en viss ip-adress motsvarar en enskild abonnent. Flera abonnenter kan dela på en och samma adress vilket medför att ip-adressen inte är synonym med den misstänktes identitet på nätet. Den stora mängden krypterad information på nätet innebär också att det kan vara svårt för brottsbekämpande myndigheter att identifiera vad som är kommunikation mellan individer i det samlade flödet.”[279]

Tanken är att detta tvångsmedel främst ska kunna användas vid misstanke om terrorbrott och annan allvarlig brottslighet.[280]

Skulle hemlig dataavläsning bli tillåten i Sverige skulle alltså användare som begår brott när de använder Tor troligtvis kunna upptäckas, samtidigt skulle tillhandahållare av Tor eventuellt kunna identifieras och därmed även möjligen undantas ansvar för eventuella brott begångna av användare eftersom det skulle framgår att tillhandahållaren inte utfört brottet.

11.4. Summering om tvångsmedel

Proportionalitetsprincipen är ett av de starkaste argumenten för att beslag och husrannsakan inte kan riktas mot tillhandahållare av Tor-noder eftersom det inte kan inhämtas någon information som kan underlätta brottsutredningar från noderna. Det är därför svårt att se något

[278] Dir. 2016:36, s. 4 f.
[279] Dir. 2016:36, s. 2 f.
[280] Dir. 2016:36, s. 6.

fall där det skulle anses proportionerligt att beslagta eller att göra en husrannsakan för att beslagta Tor-noder endast på grund av att de är Tor-noder.

Hemlig avlyssning eller övervakning av Tor-noder bör inte heller kunna utföras eftersom tillhandahållandet av Tor-noder enligt redogörelsen i Del 1inte utgör ett sådant tillhandahållande enligt LEK som möjliggör för rättsvårdande myndigheter att använda dessa tvångsmedel.

För att skydda annan information som tillhandahållare av Tor-noder behandlar i samband med tillhandahållandet går det att vidta flera åtgärder för att separera Tor-noderna från den övriga verksamheten.

11.5. Att tänka på praktiskt

För att vara på säkra sidan gällande beslag och husrannsakan i verksamheter där känslig information såsom källor eller medlemsregister hanteras ska här ges några praktiska exempel på hur sådan information kan skyddas.

- Konfigurera Tor-noderna på enheter som är helt tomma och inte används för något annat ändamål än att driva noder.
- Om enheterna är placerade i samma hus som verksamhet med känslig information, placera servrarna i ett avskilt rum avsides från den övriga verksamheten där det inte finns tillgång till någon känslig information.
- Hyr servrar i en serverhall eller liknande för att avskilja verksamhet som kan innehålla känsliga uppgifter från risken av husrannsakan och beslag av Tor-noderna.
- Se till att konfigurationen av Tor-noderna sker helt felfritt så att enheterna inte fungerar på ett oönskat sätt och exempelvis börjar lagra metadata.
- Tillhandahåll Tor-noder genom att först använda en VPN-tjänst för att minimera risken att visa Tor-nodens ip-adress och därigenom bli identifierad.

För mer information om hur du kommer igång med Tor hänvisas till IIS Internetguide #39.[281]

[281] Thoresson, Anders, *Internetguide #39 Kom igång med Tor!,* https://www.iis.se/docs/kom_igang_med-tor.pdf.

12. Internationell utblick

Genom kontakter med personer involverade i utvecklingen av Tor har erfarenheter från andra länder än Sverige kunnat inhämtas i syfte att ge en fingervisning om hur frågor gällande brott och tillhandahållande av Tor-noder har hanterats i andra länder.

I Nederländerna har det vid flertalet tillfällen skett beslag av utgångsnoder. Detta skedde dock senast i början av 2010-talet. Vid samtliga tillfällen visade det sig att den nederländska polisen inte hade kunskap om vad en Tor-nod var eller om vilken information som fanns på den. Idag har den nederländska polisen enligt uppgift tillräcklig kunskap om vad Tor-noder är och hur de fungerar för att liknande beslag inte ska förekomma. I USA har det enligt uppgift skett två beslag de senaste tio åren.

I både Nederländerna och USA har förundersökningar inletts men slutsatserna har varit att det är för dyrt och att fortsatt utredning inte skulle leda till något tillfredställande resultat varför förundersökningarna har lagts ner.

I Nederländerna greps en person vars barn tillhandahöll Tor-noder utan att föräldern visste om det. Den gripna personen misstänktes för barnpornografibrott, men släpptes inom kort från polisen och förundersökningen lades ner cirka två år efter tillslaget.

En Österrikisk medborgare dömdes dock för att ha tillhandahållit Tor-noder men detta var kopplat till att han även deltagit i distribution av barnpornografi genom sina enheter. Han hade även uppmuntrat andra att använda sig av Tor för att dela barnpornografi. Han dömdes alltså inte enbart på grund av tillhandahållandet av Tor-noderna.

Det har ännu inte offentliggjorts någon information om Tor-noder avlyssnats. Det har dock enligt uppgift förekommit att tillhandahållare av Tor-noder blivit kontaktade av myndigheter från andra länder än deras egna och blivit tillfrågade om de kan få avlyssna tillhandahållarens Tor-noder. I de fall detta har inträffat har personerna sagt nej till att låta sina noder avlyssnas. Det finns dock ingen uppgift om vilka länder det är som har ställt frågan.

Både i Australien och i Turkiet har ISP:er sagt att användare av deras tjänster inte får tillhandahålla Tor-noder om de använder ISP:ernas tjänster. Detta anses framgå av användarvillkoren. I Australien pekade ISP:erna på nationell lagstiftning medan grunden för beslutet i Turkiet var något oklart.

Det finns idag inga kända attacker mot Tor-nätverket som har lett till skador på själva nätverket, men den största risken för användare av Tor är enligt de tillfrågade personerna att de inte vidtar ytterligare anonymiseringsåtgärder för att skydda sig på internet såsom kryptering av meddelanden och liknande.

Förhoppningen för Tor-nätverket i framtiden är att ”high-latency” och ”message-based anonymization” ska bli tillgängligt för användare. Detta skulle innebära ett nästan helt separat system från dagens Tor-nätverk men förhoppningsvis skulle de existerande noderna kunna återanvändas även i det nya systemet. Det nya systemet skulle inte kunna användas för all trafik, men anonymiteten och skyddet för personer skulle öka avsevärt.

Det bör här även nämnas att en svensk medborgare under 2016 har blivit delgiven misstanke om medhjälp till bedrägeri i Turkiet. Anledningen till misstanken är att en identifierad person gjort sig skyldig till bedrägeri och då använt sig av Tor. Den svenska medborgaren tillhandahöll utgångsnoden som trafiken gick ut genom varför denne identifierades av Turkiska myndigheter. Det har i dagsläget genomförts ett förhör med den svenska medborgaren, men ingen annan information eller åtgärd har ännu vidtagits av den Turkiska staten.

13. Avslutande ord

Denna rapport har givit en överblick över de rättsliga frågor som aktualiseras vid tillhandahållande av Tor-noder. Med detta sagt återstår det att se hur Tor och liknande tjänster kommer bedömas av domstolarna. Flera frågor återstår att utredas och som endast från fall till fall kan ges ett klart svar på. Några av de frågor som i denna rapport utelämnats är om tillhandahållande av Tor-noder ska anses utgöra en tjänst eller en del av en tjänst, om tillhandahållandet är aktivt eller passivt, vilka skadeståndsrättsliga aspekter som kan uppkomma vid tillhandahållande av Tor-noder, om tillhandahållare av Tor-noder skulle kunna dömas i utvidgat medgärningsmannaskap och frågor om jurisdiktion.

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 klara svar ges förrän domstolarna har fått uttala sig.

I denna rapport har bland annat frågor om yttrandefrihet och rätten till skydd för personlig integritet berörts i relation till behovet att beivra brott på internet. Avvägningen mellan dessa intressen har inte varit föremål för denna rapport och är i slutändan en fråga för lagstiftaren och domstolarna att ta ställning till, men den väcker onekligen flera intressanta frågor.

Kan det exempelvis vara så att vi idag lever i en tid då vi får acceptera att visa brott inte kan beivras på grund av att det på internet går att dölja sin identitet? Är det så att lagstiftaren behöver ändra lagar för att motverka brott på internet och skulle det vara acceptabelt att våra fri- och rättigheter därför inskränks? Vad är vi beredda att betala för att brott ska kunna beivras och hur ska vi kunna skydda oss från att själva bli offer för brott som inte går att klara upp?

Även om det inte finns klara svar på dessa frågor finns det idag en sak som borde vara säker. Legalitetsprincipen ska fortsatt utgöra utgångspunkten för spelreglerna inom straffrätten för att de värden som ett demokratiskt samhälle bygger på ska kunna upprätthållas.

De företag och organisationer som överväger att tillhandahålla Tor-noder ska vara medvetna om att mediabilen av Tor-nätverket generellt är att Tor används av kriminella för att utföra brott. Även om det saknas faktiska uppgifter om hur stor del av trafiken i Tor som är kopplad till brottslighet eller om andelen är större än på internet i stort är detta något som riskerar att påverka synen på företaget eller organisationen negativt. Få företag eller organisationer vill

bli förknippade med brottslig verksamhet. Risken med att avskräckas av mediabilden är dock att de fri- och rättigheter som skyddas av Tor-nätverket riskerar att försummas.

Den största delen av dem som använder Tor gör det troligen för att de vill och behöver skydd för sin identitet och integritet av olika anledningar. Kanske för att de lever under förhållanden där staten bestraffar de som har en viss sexuell läggning, religion eller kritiserar staten. Det kanske är journalister som försöker skydda sina källor för att kunna sprida samhällsviktig journalistik. Det kan också vara personer som helt enkelt inte vill att företag ska kunna spåra dem för att adressera reklam baserat på deras användning av internet.

Användningsområdena för Tor är många och högst troligt i de flesta fall viktiga. Men så länge mediabilden ger allmänheten uppfattningen att nätverket syftar till att underlätta brottslighet och det saknas förtroendeingivande och publika tillhandahållare kommer skepsisen mot tillhandahållare av Tor-noder att kvarstå.

Tack!

I utarbetandet av denna rapport har följande personer i stor utsträckning deltagit med värdefulla synpunkter och utmanande diskussioner:

Daniel Westman, oberoende rådgivare inom IT- och medierätt samt doktorand vid Juridiska institutionen vid Stockholms universitet

Linus Nordberg, utvecklare på Sunet samt ledamot i Föreningen för Digitala Fri- och Rättigheter (DFRI)

Fredrik Engström, advokat på Engström & Hellman Advokatbyrå

Källförteckning

Juridisk litteratur

Nordh, Roberth, Tvångsmedel: kvarstad, häktning, beslag, husrannsakan m.m., Iustus, Uppsala, 2007

Ekelöf, Per Olof, Edelstam, Henrik & Heuman, Lars, Rättegång. H. 4, 7., omarb. och rev. uppl., Norstedt, Stockholm, 2009

Zila, Josef, Brottsbalk (1962:700) 23 kap. 4 §, Lexino 2012-07-01

Lindberg, Gunnel, Straffprocessuella tvångsmedel: när och hur får de användas?, 3., [rev.] uppl., Karnov Group, Stockholm, 2012

Holmqvist, Lena, Leijonhufvud, Madeleine, Träskman, Per Ole och Wennberg, Suzanne (red.), Brottsbalken: en kommentar. Del 2, (13-24 kap.): brotten mot allmänheten och staten m.m., 7., [omarb.] studentutg., Norstedts juridik, Stockholm, 2013

Asp, Petter och Ulväng, Magnus, Kriminalrättens grunder, 2., omarb. uppl., Iustus, Uppsala, 2013

Stålhandske, Jan, Kommentar till Lag (2002:562) om elektronisk handel och andra informationssamhällets tjänster, Karnov, 2015-04-01

Lindberg, Gunnel, Rättegångsbalk (1942:740) 27 kap. 1 §, Lexino 2015-07-01

Nilsson, Göran, Brottsbalk (1962:700) 17 kap. 11 §, Lexino 2015-08-01

Juridiska artiklar

Jareborg, Nils, Påföljdsbestämningens struktur, SvJT 1992 [s.258-275]

Asp, Petter och Ulväng, Magnus, Täckningsprincipens ABC, Juridisk publikation Nummer 02/2009, [s. 265-273], Stockholm, 2009, http://juridiskpublikation.se/wp-content/uploads/2014/10/22009_Petter-Asp-Magnus-Ulv%C3%A4ng.pdf

Nicander, Hans, Upphovsrätten och medverkansansvaret i en digital miljö, SvJT 2012 [258-281]

Offentligt tryck

Kommittédirektiv

Kommittédirektiv 2016:20, Moderna regler om beslag och husrannsakan

Kommittédirektiv 2016:36, Hemlig dataavläsning

Statliga offentliga utredningar

SOU 1944:69, Lagstiftning om brott mot staten och allmänheten

SOU 1988:7, Frihet från ansvar-Om legalitetsprincipen och allmänna grunder för ansvarsfrihet

SOU 1995:47, Tvångsmedel enligt 27 och 28 kap. RB samt polislagen, Slutbetänkande av Polisrättsutredningen

SOU 1996:185, Straffansvarets gränser Del 1, Betänkande från Straffansvarsutredningen

SOU 2001:28, Yttrandefrihetsgrundlagen och Internet. Utvidgat grundlagsskydd och andra frågor om tryck- och yttrandefrihet

SOU 2002:60, Lag om elektronisk kommunikation

Departementspromemorior

Ds 2005:6, Brott och brottsutredning i IT-miljö. Europarådets konvention om IT-relaterad brottslighet med tilläggsprotokoll

Ds 2014:23, Datalagring EU-rätten och svensk rätt

Propositioner

Proposition 2001/02:150, Lag om elektronisk handel och andra informationssamhällets tjänster, m.m

Proposition 2002/03:110, Lag om elektronisk kommunikation, m.m

Proposition 2005/06:59, Företagsbot

Proposition 2005/06:195 Elektroniska kommunikationstjänster m.m. inom psykiatrisk tvångsvård

Proposition 2010/11:46, Lagring av trafikuppgifter för brottsbekämpande ändamål - genomförande av direktiv 2006/24/EG

Proposition 2011/12:55, De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation

Rättsfall

Sverige

Tingsrätt

Mål nr B 13301-06, Stockholms tingsrätt, 2009-04-17

Mål nr B 4754-11, Skaraborgs tingsrätt, 2012-03-27

Mål nr T 15142-14, Stockholms tingsrätt, 2015-11-27

Mål nr B 1687-14, Attunda tingsrätt, 2016-06-23

Hovrätt

RH 1999:84, RH 2009:30, RH 2009:41,

Mål nr B 4041-09, Svea Hovrätt, 2010-11-26

RH 2011:54

RH 2013:7

RH 2013:13

Mål nr B 3117-13, Svea hovrätt, 2013-10-31

RH 2015:40, Svea hovrätt, 2015-03-05

Mål nr B 6051-15, Svea hovrätt, 2015-09-09

Mål nr B 5801-15, Svea hovrätt, 2016-03-01

Mål nr B 2932-16, Svea hovrätt, 2016-03-30

Högsta domstolen

NJA 1963 s. 574

NJA 1984 s 922

NJA 1988 s. 383

NJA 1991 s. 783

NJA 1996 s. 79

NJA 1999 s. 87

NJA 1999 s. 561

NJA 2001 s. 579

NJA 2003 s. 473

Mål nr B 1471-13, Högsta domstolen, 2015-03-04

NJA 2006 s. 577

NJA 2007 s. 369

NJA 2007 s. 929

NJA 2009 s. 599

NJA 2012 s. 826

NJA 2014 s. 139

NJA 2015 s. 501

NJA 2015 s. 631

Specialdomstol

MÖD 2001:22

MÖD 2001:23

MÖD 2001:24

EU

Mål C-236/08, Google France SARL, Google Inc v. Louis Vuitton Malletier SA.

Mål C-324/09, L’Oréal SA m.fl v. eBay International AG m.fl.

Mål C-293/12 och C-594/12 Digital Rights Ireland och Seitlinger m.fl. mot Minister for Communications m.fl

Författningar samt bilagor

Sverige

Tryckfrihetsförordning (SFS 1949:105)

Kungörelse om beslutad ny regeringsform (SFS 1974:152)

Yttrandefrihetsgrundlag (SFS 1991:1469)

Rättegångsbalk (SFS 1942:740)

Brottsbalk (SFS 1962:700)

Miljöbalk (SFS 1998:808)

Lag om straff för vissa trafikbrott (SFS 1951:649)

Lag om upphovsrätt till litterära och konstnärliga verk (SFS 1960:729)

Narkotikastrafflag (SFS1968:64)

Lag (SFS 2002:562) om elektronisk handel och andra informationssamhällets tjänster

Lag om straff för terroristbrott (SFS 2003:148)

Lag (SFS 2003:389) om elektronisk kommunikation

Lag om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet (SFS 2010:299)

Lag (SFS 2012:127) om ändring i lagen (SFS 2003:389) om elektronisk kommunikation

EU

Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna

Europeiska unionens stadga om de grundläggande rättigheterna (2010/C 83/02)SV 30.3.2010 Europeiska unionens officiella tidning C 83/389

Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden

Europaparlamentets och rådets direktiv 2002/19/EG av den 7 mars 2002 om tillträde till och samtrafik mellan elektroniska kommunikationsnät och tillhörande faciliteter

Europaparlamentets och rådets direktiv 2002/20/EG av den 7 mars 2002 om auktorisation för elektroniska kommunikationsnät och kommunikationstjänster

Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster

Europaparlamentets och rådets direktiv 2002/22/EG av den 7 mars 2002 om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster

Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation

Europaparlamentets och rådets beslut nr 676/2002/EG av den 7 mars 2002 om ett regelverk för radiospektrumpolitiken i Europeiska gemenskapen (radiospektrumbeslut)

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

Kommissionens förslag till direktiv om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster, KOM(2000) 393, EGT C 365 E, 19.12.2000

Elektroniskt material

Information om Tor

Officiell hemsida för Tor, https://www.torproject.org/

Officiell hemsida för Tor, information om bryggnoder, https://www.torproject.org/docs/bridges.html.en

Officiell hemsida för Tor, ”hidden services”, https://www.torproject.org/about/overview.html.en#hiddenservices

Officiell hemsida för Tor, ”Frequently used terms”, https://metrics.torproject.org/about.html

Officiell lista av finansiärer av Tor, https://www.torproject.org/about/sponsors.html.en

Officiell hemsida för Tor, consensus och dess statistik, https://consensus-health.torproject.org/

Officiell hemsida för Tor, FAQ, https://www.torproject.org/docs/faq.html.en#ExitPolicies

Officiell hemsida för Tor, 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

Översikt av Tor, https://www.torproject.org/about/overview

Meddelande om lansering av ”onion router”, 20 september 2002, http://archives.seul.org/or/dev/Sep-2002/msg00019.html

Meddelande om lansering av Tor, 8 oktober 2003, https://lists.torproject.org/pipermail/tor-dev/2003-October/002185.html

LevineOn Yasha, Almost everyone involved in developing Tor was (or is) funded by the US government, Panodaily, den 16 juli 2014, http://pando.com/2014/07/16/tor-spooks/

Hemsida om ”onion routing”, historisk exposé, http://www.onion-router.net/History.html

Rapporter m.m.

Vilka tjänster och nät omfattas av LEK? En vägledning, PTS-ER-2009:12, 2009-03-11, http://www.pts.se/upload/Rapporter/Internet/2009/ekomtjanster-2009-12.pdf

It-relaterade brott - polisens arbete, senast uppdaterad den 8 december år 2014 kl. 15:54, https://polisen.se/Om-polisen/Olika-typer-av-brott/IT-brott/

Edström, Martin och Fridh Kleberg, Carl, Anonymitet och kryptering–tips till journalister, https://www.iis.se/docs/Anonymitet-och-kryptering-%E2%80%93-tips-till-journalister.pdf

Andersson Sus, Laurin Fredrik och Jankov Petra, Digitalt källskydd – en introduktion, , https://www.iis.se/docs/digitalt-kallskydd-2.pdf

Thoresson, Anders, Internetguide #39 Kom igång med Tor!, https://www.iis.se/docs/kom_igang_med-tor.pdf

Trehörning, Pär, Officiell presentation av yttrandefrihetsgruppen, https://www.sjf.se/yrkesfragor/yttrande-tryckfrihet/yttrandefrihetsgruppen

Artiklar

MacAskill, Ewen och Ackerman, Spencer, NSA collecting phone records of millions of Verizon customers daily, The Guardian, den 6 juni år 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Pouls, Kevin, *The FBI Used the Web's Favorite Hacking Tool to Unmask Tor Users*, Wired, den 16 december år 2014, http://www.wired.com/2014/12/fbi-metasploit-tor/

Paganini, Pierluigi, *Who hacked a cluster of Tor servers in the Netherlands?*, blog Security affairs, den 24 december 2014, http://securityaffairs.co/wordpress/31429/hacking/who-hacked-a-cluster-tor-servers.html

Carr, Paul, *If you still trust Tor to keep you safe, you're out of your damn mind*, Panodaily, den 26 december år 2014, http://pando.com/2014/12/26/if-you-still-trust-tor-to-keep-you-safe-youre-out-of-your-damn-mind/

FBI stängde ökänd drog- och vapenhandelssajt, Bie, Nanok, 2 oktober 2013, uppdaterad 9 oktober 2013, http://www.svt.se/nyheter/utrikes/okanda-drog-och-vapenhandelssajten-silk-road-nedstangd.

Digitala uppslagsverk

Wikipedia om Deep web, https://sv.wikipedia.org/wiki/Deep_web

Wikipedia om Darknet, https://sv.wikipedia.org/wiki/Darknet

Wikipedia om krypteringssystemet Diffie–Hellman, https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange#Description