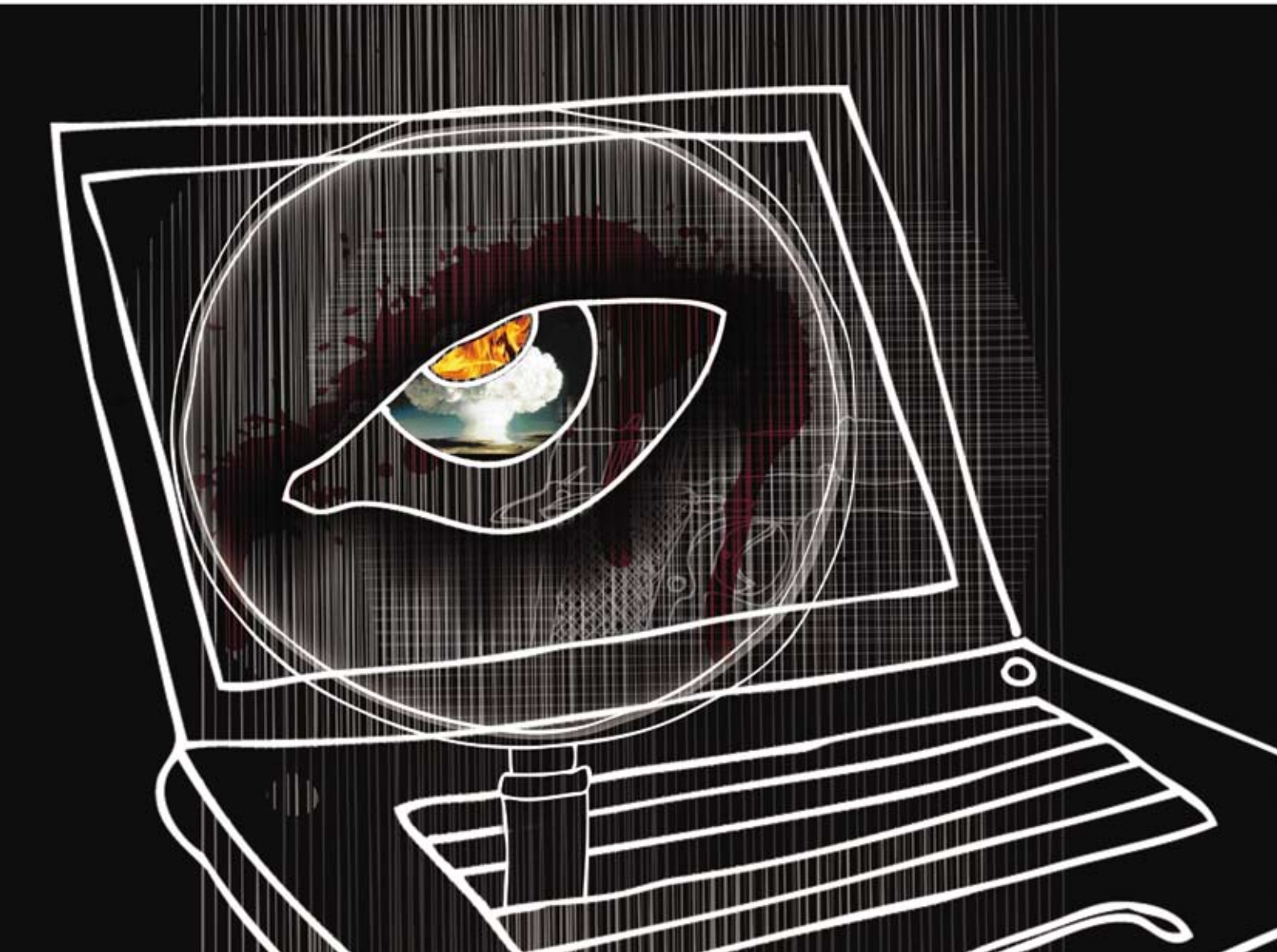
Anders R Olsson

Sökes: En teknisk lösning på ondskans problem

En guide om filtrering av innehåll på nätet



Sökes: En teknisk lösning på ondskans problem

.SE:s Internetguide, nr 17
Version 1.0 2010

Författare: Anders R Olsson
Redaktör: Lennart Bonnevier
Formgivning, layout och redigering: Gunnel Olausson/FGO AB
Illustrationer: © Camilla Laghammar
Första upplagan, första tryckningen.
Tryck: Danagårds Grafiska, Ödeshög, februari 2010.
ISBN: 978-91-978350-6-0

.SE (Stiftelsen för Internetinfrastruktur) ansvarar för Internets svenska toppdomän. .SE är en oberoende allmännyttig organisation som verkar för en positiv utveckling av Internet i Sverige.

Besöksadress: Ringvägen 100 A, 9 tr, Stockholm
Brevledes på .SE Box 7399, 103 91 Stockholm
Telefon: +46 8 452 35 00
Fax: +46 8 452 35 02
E-post: info@iis.se
Organisationsnummer: 802405-0190
www.iis.se

Förord

Trycket på Internet ökar fortlöpande. Inte bara trycket i kvantitativ mening att användarna blir allt fler och att mängden kommunicerat material växer utan också det politiska trycket. För demokratins skull behöver vissa frågor få tydliga svar. Vem ska övervaka nätet? Med vilka metoder ska det ske? Var ska gränsen för det tillåtna gå? Hur ska rättsväsendet ingripa mot det som har förbjudits?

Filtrering är kanske, med tanke på hur starka censureffekter som kan åstadkommas, det ingripande på Internet som idag behöver uppmärksammas mest. Här står det uppenbarligen och väger. Det är inte bara i Kina och Iran som statsmakten utnyttjar denna möjlighet att ingripa. Också för västvärldens lagstiftare och internetoperatörer är frestelsen att filtrera stark. Krav på filtrering av olagligt, skadligt eller upprörande material har rests i många sammanhang, och i några har filtreringsanhängarna fått gehör. Någon ordentlig utredning eller politisk debatt i ämnet har vi dock inte sett. Vi behöver bådadera innan filtrerandet börjar sprida sig på allvar i Sverige och andra EU-länder.

Ett stort tack till stiftelsen .SE som gett mig möjlighet att under hösten 2009 skriva denna guide om filtrering. Den aktualiserar grundläggande demokratifrågor, och även om den mera har karaktär av upplysnings- än debattskrift skymtar författarens åsikter naturligtvis igenom på vissa ställen. De är alltså mina, och behöver inte på varje punkt överensstämma med .SE:s uppfattning.

Hässelby i februari 2010
Anders R Olsson

Hjälp oss att förbättra
Om du hittat fel eller har synpunkter på denna guide kan du sända dem till publikationer@iis.se

Inledning

Ska Internetoperatörerna filtrera bort innehåll – censurera nätet – för användarna? Varje demokrat har ett spontant svar på den frågan.

Saken visar sig dock, vid närmare betraktande, vara mer komplicerad än man kan tro. På ett principiellt plan väljer vi naturligtvis ickefiltrering framför filtrering, precis som vi väljer frihet framför ofrihet, men därmed har vi inte besvarat någon av de svåra frågorna.

För det första måste man ta ställning till vem som överhuvudtaget ska fatta beslut om filtrering. Är det en fråga för lagstiftaren, eller är det något som operatörerna och deras kunder ska klara ut på en fri marknad, utan statliga ingrepp? Är Internetuppkoppling bara en teknisk tjänst bland andra, som ett el- eller telefonabonnemang, eller har Internet blivit en för samhället så viktig arena att lagstiftaren måste bestämma – för att säkra att medborgarna kan utöva sina fri- och rättigheter – vad operatörerna får och inte får göra?

För det andra måste man, när man tar principiell ställning mot filtrering, diskutera frågan om undantag. Också friheten måste ha gränser. Min frihet får inte vara en frihet att skada andra. Om alla de yttrandefrihetsbrott lagboken rymmer är befogade kan diskuteras, men några är det definitivt. Att förtala människor, sprida barnpornografi eller avslöja statshemligheter kan inte bli tillåtet bara därför att det sker via Internet.

”Att förtala människor, sprida barnpornografi eller avslöja statshemligheter kan inte bli tillåtet bara därför att det sker via Internet.”

Det faktum att yttranden kan skada och utgöra brott leder naturligtvis till politiska krav på övervakning av – och ingrepp i – informationsströmmarna på Internet. Det ”fria” och ”gränslösa” nätet öppnar visserligen för allt möjligt gott – en mänsklig, social och ekonomisk utveckling som alla bejakar – men också för det onda. *Vad* som egentligen är så ont att det måste bekämpas och *hur det ska gå till* behöver alltid diskuteras, men *att* det onda ska kunna bekämpas i demokratiskt acceptabla former är självklart.

Filtrering är en form av bekämpande – en möjlighet att censurera Internet som redan har börjat användas. Den är dock inte demokratiskt beslutad och behöver snarast granskas, diskuteras närmare

– och placeras i ett större sammanhang. Syftet med denna guide är att bidra till att så sker.

För beslutsfattare världen över framstår nu filtrering av farligt, skadligt eller av andra skäl olämpligt (för någon med inflytande) Internetmaterial som ett realistiskt alternativ. *”Den framväxande trenden är alltmer filtrering på alltfler platser, med användning av tekniker som med tiden blir alltmer sofistikerade. Denna trend utvecklas i en tid när alltfler människor på alltfler platser använder Internet för ändamål som är allt viktigare i deras liv.”* (Forskarna Jonathan Zittrain och John Palfrey i boken *Access Denied 2008*. Egen översättning)

Den som lutar sig tillbaka och betraktar frågan om ”friheten på Internet” ur ett bredare perspektiv finner att nationalstaterna nu försöker etablera en rättslig kontroll över medborgarnas agerande på Internet som kan liknas vid den man utövar i den fysiska världen. Många kritiker av denna trend hävdar, med väl underbyggda argument, att den polisiära kontrollen online snarast tycks bli hårdare än den någonsin varit IRL, det vill säga i den fysiska världen. Därmed blir den mer kontroversiell och mer problematisk ur demokratisk synvinkel.

En svensk som före Internets genombrott hade föreslagit att staten skulle ges både rätt och praktisk möjlighet att öppna och läsa alla pappersbrev som medborgarna skickade till varandra hade avfärdats som kommunist, fascist eller bara dåre. Idag har, med den så kallade FRA-lagen, just en sådan ordning etablerats för e-post. En överväldigande riksdagsmajoritet har dock varit överens om kursändringen. Initiativet togs av den socialdemokratiska regering som avgick 2006 och FRA-beslutet genomdrevs sedan i riksdagen av de fyra borgerliga partier som övertog regeringsmakten.[1] Det som kännetecknar vår tid är alltså inte bara en snabb teknisk utveckling, utan också stora förskjutningar i medborgarnas föreställningar om vad som är rimligt i relationen mellan medborgare och

1 Detta är bara ett exempel av många på hur sedan länge etablerade föreställningar om medborgerliga fri- och rättigheter har omvärderats i övergången till det så kallade IT-samhället. Frågan behandlas mer utförligt i Anders R Olssons bok *Att stänga det öppna samhället*, Tusculum förlag 2008.

stat. En statlig insyn i medborgarnas privata förhållanden som länge varit politiskt omöjlig har nu blivit möjlig. Mindre partier i och utanför riksdagen protesterar energiskt, men de tycks förbli små partier.

Betraktar vi alternativen för den politiske beslutsfattare i Sverige som har ambitionen att påverka informationsflöden på Internet finner vi att de är många. Ingen metod för påverkan är riktigt effektiv, men de kan användas med hyggligt genomslag och med flera metoder sammantagna blir effekten stark.

Nationalstaterna utövar vanligen sin makt över nätet via mellanhänder. Sådana finns det många. Internet förutsätter elektricitet, kablar, servrar, sökmotorer, bank- och betaltjänster och mycket mer. All denna utrustning och alla dessa tjänster kontrolleras av företag som i sin tur måste underordna sig nationalstaters lagar. Företag har små möjligheter att motsätta sig myndighetsbeslut i de länder där de bedriver verksamhet.

”Nationalstaterna utövar vanligen sin makt över nätet via mellanhänder. Sådana finns det många.”

Det är, för att exemplifiera, skälet till att den föregivet gränslösa e-handeln inte har fått så revolutionerande effekter som många förutspådde för tio år sedan. Visst förändras nu handelns villkor, påpekar forskarna Jack Goldsmith och Tim Wu[2], men det sker inte okontrollerat.

När amerikanska tobaksföretag via nätet började sälja cigaretter billigt från skattebefriade indianreservat ingrep USA:s regering. Med hänvisning till att man vid tobaksförsäljning online inte effektivt kontrollerade köparnas ålder förbjöds verksamheten, men inte genom krav på de säljande företagen utan genom påtryckningar på kreditkortsföretag som Visa och MasterCard. ”Slutar ni inte acceptera betalning för dessa cigaretter får ni ta konsekvenserna” var regeringens besked. Cigaretthandeln över nätet krympte genast till ett minimum.[3] En liknande aktion 2009 var bildandet av en ”finansiell koalition” mellan svenska banker i syfte att försvåra handeln

2 Goldsmith, Jack/Wu, Tim. *Who Controls the Internet? Illusions of a Borderless World.* Oxford University Press, 2006.

3 Goldsmith, Jack/Wu, Tim 2006, sid 76–77.

med barnpornografi. Bankerna spärrar helt enkelt betalning till vissa Internetsidor där besökare kan köpa och ladda ner barnpornografiskt material.[4]

Mellanhänder – Internetoperatörer, banker och kreditkortsföretag till exempel – kan alltså frivilligt eller på statens order påverka en del av det som sker på nätet. Lagstiftaren har fler möjligheter. Utan anspråk på att täcka in alla kan följande alternativ nämnas:

1. **Att kriminalisera vissa yttranden och viss information**. Förbud mot yttranden finns i alla med Sverige jämförbara länder och gäller sådant som vi kallar förtal, uppvigling, hets mot folkgrupp, olaga hot med mera. Det är lagstiftarens klassiska metod att begränsa yttrandefriheten. Staten ingriper vanligen efter att brott har begåtts och försöker då finna och lagföra de skyldiga. Samtidigt är avsikten med förbuden naturligtvis också att avskräcka från yttrandefrihetsbrott.

2. **Att vidga det straffbara området för olika sorters underlättande av/förberedelser för/medverkan till brott**. Ett exempel på detta är förbudet, infört i Sverige 2009, mot så kallad grooming. Det brottet tar sikte på kontakter med barn, till exempel via Internet, som kan leda till sexuella övergrepp vid ett senare möte med barnet. (Med barn menas här personer under 15 år.) Ett annat exempel är den *”lag om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet”* som den svenska regeringen ska införa för att leva upp till åtaganden som följer av en Europarådskonvention från 2005 och ett rambeslut i EU 2008 om bekämpande av terrorism. Förslag till en sådan lag överlämnades till Lagrådet i december 2009 och innebär bland annat att den person ska straffas som *”meddelar eller söker meddela instruktioner om tillverkning eller användning av sådana sprängämnen, vapen eller skadliga eller farliga ämnen som är särskilt ägnade att användas för särskilt allvarlig brottslighet, eller om andra metoder eller tekniker som är särskilt ägnade för sådant ändamål, om gärningen har begåtts med vetskap om att instruktionerna är avsedda att användas för särskilt allvarlig brottslighet”.*

4 Polisens pressmeddelande 2009-06-23. Se: www.polis.se

3. **Att kriminalisera Internetanvändarnas själva befattning med viss typ av information**. Ett sådant förbud gäller barnpornografi. Ett annat tar sikte på personuppgifter. Den svenska Personuppgiftslagen, som i huvudsak är en översättning av ett EU-direktiv[5], stadgar att hantering av personuppgifter är förbjuden och medger sedan vissa undantag. Ytterligare ett förbud kallas dataintrång, riktat mot den som *"olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling"* (brottsbalken 4:9 c). Det är alltså generellt förbud mot att titta på elektroniskt lagrad information utan "ägarens" tillåtelse – en av de märkligaste och mest svårtolkade bestämmelserna i svensk lag. (Sådana brott, där det straffbara är att inneha eller befatta sig med information, är en sentida uppfinning. De fanns överhuvudtaget inte för 20 år sedan.)

4. **Att sprida det rättsliga ansvaret för olagliga yttranden eller olaglig hantering av data** till fler än de egentliga gärningsmännen eller – om det är en grundlagsskyddad publicering – den ansvarige utgivaren. En person som har en webbplats där besökare kan skriva eller bidra med material kan enligt den så kallade BBS-lagen göras ansvarig för materialet om han/hon inte tar bort det tillräckligt snabbt. Den som bedriver en verksamhet på nätet som underlättar för andra att begå brott kan under vissa omständigheter dömas för medverkan till brotten. (Pirate Bay-målet är ett exempel.)

5. **Att stänga av enskilda och företag som misskött sig från Internet**. Diskussionerna 2008–2009 om EU:s så kallade telekompaket har handlat bland annat om detta. Avstängning kan ske genom domstols- eller myndighetsbeslut. Frankrike har redan infört sådan lagstiftning (HADOPI), och liknande bestämmelser förbereds vid årsskiftet 2009/2010 i fler länder (Se kapitlet Vad är det onda som ska bort?). Ett alternativ är att Internetoperatörerna – frivilligt eller under press från myndigheter – stänger av kunder.

5 Dir. 95/46/EG

6. **Att övervaka Internet**. Det kan i Sverige ske via Försvarets Radioanstalt, FRA, eller något polisiärt organ. De möjliga metoderna är flera. Det må vara svårt att studera och därmed svårt att bevisa, men det är inget djärvt antagande att en långtgående övervakning får avskräckande effekter på många nätanvändare – på betydligt fler än de brottslingar som övervakningen officiellt är till för att skydda mot.

7. **Att vidga möjligheterna för enskilda och företag att driva rättsprocesser mot varandra**. Det kan gälla upphovsrättsliga intrång, där musikförlag stämmer enskilda fildelare med stöd i den så kallade IPRED-lagen, eller personliga kränkningar där medborgare A vill stämma medborgare B för förtal eller andra oförrätter.

I samtliga sju fall är ett av syftena med lagstiftningen att avskräcka från olagligt eller oönskat beteende.

För politiker och andra beslutsfattare har dessa alternativ för- och nackdelar av olika slag beroende på sammanhanget. De tillämpas i olika utsträckning i olika delar av världen och aktualiserar rader av etiska, politiska, juridiska, tekniska och praktiska frågor – som inte närmare ska behandlas här. Denna guide fokuserar istället på ett åttonde alternativ: filtrering, det vill säga att med tekniska åtgärder försöka blockera information/dataströmmar för alla medborgare i en stat eller ett geografiskt område.

Som metod för maktutövning har filtrering en rad fördelar för de politiska ledare som överväger att ingripa på Internet. Filtrering fordrar ingen användning av statens våldsmonopol, det vill säga att människor spärras in eller utsätts för direkt tvång på annat sätt. Filtrering kan vara dold – det är ofta svårt för medborgarna att upptäcka att de faktiskt är utsatta för censur. Filtrering kan vid en starkt formalistisk tillämpning av regler om yttrandefrihet anses tillåten eftersom den inte utgör hinder för enskilda att yttra sig, den försvårar bara för andra att lyssna. (Hårklyverier, kan tyckas, men sådana kan vara svåra att undvika när lagar ska tillämpas.) Sist men inte minst kan ansvaret för filtrering skjutas över på andra aktörer än politikerna själva. Det finns inga lagregler eller politiska beslut om den filtrering av barnpornografi som pågår i Sverige. De

”Filtrering kan … anses tillåten eftersom den inte utgör hinder för enskilda att yttra sig, den försvårar bara för andra att lyssna.”

stora Internetoperatörerna valde 2005 att frivilligt filtrera enligt polisens önskemål, men ”frivilligheten” uppstod inte förrän dåvarande justitieministern Bodström hotat dem med tvingande lagstiftning.[6]

Det finns också nackdelar. En någorlunda heltäckande filtrering förutsätter att många Internetoperatörer tvingas eller övertygas om att filtrera, vilket kan vara svårt. Det så kallade filtret blir aldrig hundraprocentigt effektivt. Det kan kringgås eller överlistas av tekniskt kunniga nätanvändare. Krypterade dataflöden kan inte filtreras. Den bristande precisionen är också ett problem – med all filtrering följer överblockering och underblockering, det vill säga filtret tar bort mer än avsett men missar samtidigt en del av det man försöker komma åt.

”Det så kallade filtret blir aldrig hundraprocentigt effektivt. Det kan kringgås eller överlistas av tekniskt kunniga nätanvändare.”

Filtrering på Internet är inte någon tekniskt enkel åtgärd. För varje form av kommunikation (e-post, webbsurfning, fildelning med flera) krävs olika slags blockerande insatser och för varje form finns flera metoder att välja på. Dock krävs alltid att operatören satsar resurser – tid och pengar – på att genomföra filtreringen. Det finns inget Internetfilter med en enkel på- och av-knapp.

Ett mer principiellt problem är att filtreringsproceduren inte kan vara öppen. Ju mer information Internetanvändarna kan få om hur filtreringen går till, desto lättare får de att undvika den. Hemlighetsmakeri är nödvändigt även om filtreringen är beslutad i god demokratisk ordning. Därmed blir det svårt eller omöjligt för medborgarna att bedöma om den utförs på ett rimligt sätt, om den får oförutsedda konsekvenser eller om den missbrukas.

Yttrandefrihetsperspektivet

Att fokus här ligger på heltäckande filtrering innebär att det mer lokala filtrerandet faller utanför guidens tema, till exempel föräldrars blockerande av information i hemmets dator, liksom bibliotek, skolors och företags filtrerande i egna datorer.

6 Dagens Nyheters nätupplaga 2005-03-11.

Ett visst mått av heltäckande filtrering har vi alltså redan. Än så länge filtreras i Sverige, så gott det går, dels skräppost och skadlig kod, vilket är nödvändigt för att Internet ska fungera väl som tekniskt system, dels barnpornografi. De intressanta frågorna handlar om *vad* som ska filtreras, *hur* beslut om filtrering ska fattas och hur den praktiskt ska *genomföras* utan att yttrande- och informationsfriheterna inskränks mer än vad som är absolut nödvändigt. Utgångspunkten måste enligt författarens uppfattning vara att värna just dessa medborgerliga friheter. Våra grundlagar (tryckfrihetsförordningen, yttrandefrihetsgrundlagen) och flera internationella konventioner som Sverige har anslutit sig till avser att garantera dem.

Det är alltså Sverige och länder med jämförbart parlamentariskt styrelseskick som kommer att stå i centrum. Att diktaturer och stater med ett utpräglat auktoritärt styre filtrerar Internet är allmänt bekant. Det kritiseras återkommande av politiska debattörer och medborgarrättsaktivister i alla delar av världen och kartläggs fortlöpande av forskare. (Särskilt inom forskningsprojektet *The Open Net Initiative*, ONI, pågår sådan kartläggning. Se kapitlet Vad är det onda som ska bort?) I diktaturer är filtrerandet i många fall så omfattande att det aldrig skulle accepteras i till exempel europeiska eller nordamerikanska länder. Beskrivningar och analyser av det som sker i Kina eller Saudiarabien har därmed liten relevans för de politiska beslut som förr eller senare behöver fattas i Sverige.

”I diktaturer är filtrerandet i många fall så omfattande att det aldrig skulle accepteras i till exempel europeiska eller nordamerikanska länder.”

De motiv som åberopas för att även i vårt land filtrera Internet är många och väsenskilda. Förslag om ytterligare filtrering har framförts både från den s-regering som avgick 2006 och den borgerliga fyrpartiregering som sedan tog över, liksom från statliga utredningar och intresseorganisationer av olika slag. Av lätt insedda skäl betraktas dock frågan som politiskt känslig, en uppfattning som säkerligen förstärktes med Piratpartiets framgång i valet till EU-parlamentet sommaren 2009. Ingen regering, inget enskilt parti har utarbetat något som kan kallas en filtreringspolitik, det vill säga har principiellt uttalat sig om vad staten ska göra eller inte göra, tillåta eller inte tillåta i detta avseende.

Filtreringsfrågan är alltså svårhanterlig. Politikers tveksamhet inför att lägga fast en tydlig linje i fråga om statliga ingripanden

på Internet är beklaglig men också i viss mån begriplig. En sådan linje förutsätter att man låser sig för framtiden, att man tar ställning i frågor om vad som mer exakt menas med demokrati, om yttrande- och informationsfriheternas värde avvägt mot andra intressen, och om vuxnas ansvar för vad barn och ungdomar ser och upplever. I en snabbt föränderlig värld – såväl medietekniskt som opinionsmässigt – är det uppenbarligen riskabelt att som ledande politiker uttala sig kategoriskt i sådana ämnen. I den positionen måste man vara för allt gott (yttrandefrihet, personlig integritet, effektiv brottsbekämpning) och mot allt ont (förtal, stöld, sexuella övergrepp) och vad som i olika situationer ska tillåtas väga tyngst kan skifta från en dag till en annan.

”Omtanken om barn och ungdomar står ofta i centrum när filtrering diskuteras. Att unga helst borde skyddas från delar av Internet … anser nog de flesta.”

Omtanken om barn och ungdomar står ofta i centrum när filtrering diskuteras. Att unga helst borde skyddas från delar av Internet – med hårdporr, grovt våld, drogpropaganda, bombrecept eller instruktioner om hur självmord utförs – anser nog de flesta. Samtidigt är det idag svårare än någonsin för vuxenvärlden att kontrollera vad barn och ungdomar exponeras för. På Internet går det inte att utöva kontroll genom åldersgränser som man gör på biografer och i porrbutiker. På nätet finns ”vuxenmaterialet” tillgängligt dygnet runt, inte som i teve på sen kvällstid när barnen har lagt sig. Dessutom är det ett faktum att många barn och ungdomar (eller åtminstone någon de känner) behärskar Internetteknologier bättre än föräldrarna. Lokal filtrering riskerar därmed att bli ineffektiv, varvid filtrering på högre nivå i systemet – hos operatörerna – framstår som det mest lockande alternativet.

En för guiden relevant distinktion är den mellan att blockera innehåll, som till exempel pornografi, och att blockera tekniska tjänster som till exempel IP-telefoni eller fildelning. I de länder där telefoni via Internet blockeras sker det i syfte att skydda nationella telebolag från konkurrens. Då handlar det dock om ekonomisk politik.

Med blockering av webbplatser som Pirate Bay, som underlättar för enskilda Internetanvändare att dela filer med varandra, är det mer komplicerat. Fildelning som sådan kan fylla viktiga funktioner och är inte olaglig i sig. Det är när den används för att sprida upp-

hovsrättsligt skyddat material som kontroverserna uppstår – och kraven på att webbplatser av Pirate Bays typ ska blockeras för Internets användare. Under förutsättning att man accepterar att upphovsrätt är något viktigt (och det gör författaren till denna guide) blir problemet då främst överblockeringen. Att blockera en webbplats med hänvisning till att majoriteten av dess besökare använder den för att göra något otillåtet innebär en kränkning av den laglydiga minoritetens yttrande- och informationsfriheter. Fildelning av material som inte har upphovsrättsligt skydd, och av material där rättighetsinnehavarna godtar spridningen, förhindras ju också. Ansträngningarna att filtrera med hänvisning till upphovsrätt, vilket det finns flera exempel på, kommer därför att behandlas i guiden.

Det behöver knappast understrykas att en text som handlar om maktutövning via Internet kan betraktas som aktuell bara under en begränsad tid. Den politiska och tekniska utvecklingen går snabbt. Vilken aktör som kommer att kunna göra vad med informationsflöden på Internet om tio år är meningslöst att spekulera om. Författarens ambition är snarast att diskutera vad som kan och bör göras de närmaste fem-sex åren.

Idag riktas kraven på filtrering – och argumenten för att man bör avstå – främst mot politiker på nationell nivå. De har i sin tur, om och när de fattar beslut om filtrering, egentligen bara en sorts aktörer att ställa krav på: Internetoperatörerna. Dels är det i praktiken bara operatörerna som med någon större effektivitet kan blockera delar av Internet för medborgarna, dels finns de så att säga inom räckhåll för lagen. De enskilda användare som sprider anstötligt (i någon mening) material via Internet är ofta svåra att identifiera, svåra att nå eftersom de kan bo var som helst i världen och svåra att ingripa rättsligt mot eftersom det inte alltid är klart vilket lands lagar som ska tillämpas. Internetoperatörerna däremot, är lätt identifierbara företag med anställda och tillgångar i det land där lagstiftaren beslutar. Åläggs dessa företag att göra något – det må vara att betala skatt eller filtrera – måste de lyda för att överleva som företag.

Privatägda företag – Internetoperatörerna – äger och kontrollerar således den arena på vilken medborgarna realiserar sina fri- och

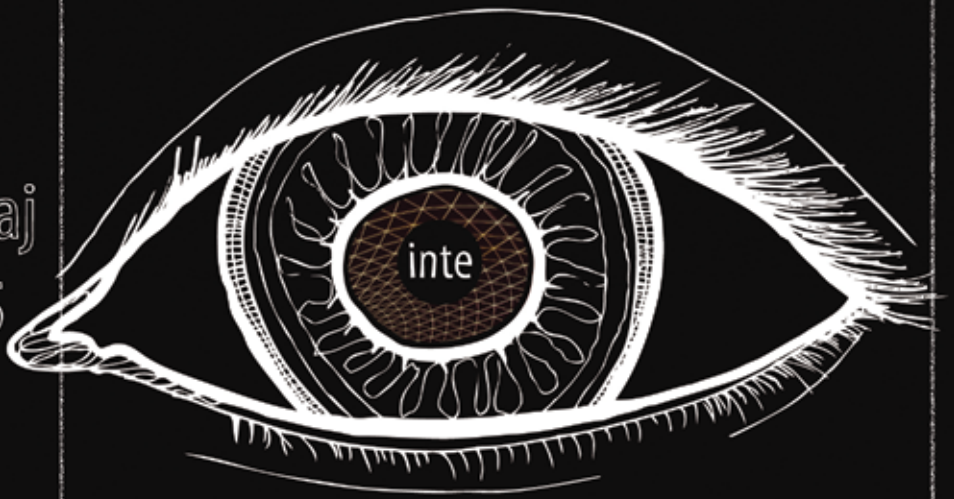
rättigheter. Vad yttrandefriheten beträffar innebär det risker av åtminstone tre slag. För det första kan operatörerna alltså bli statsmaktens redskap för att i smyg och/eller med utomrättsliga metoder inskränka denna frihet. För det andra kan operatörerna få egna, företagsekonomiska incitament för att styra eller blockera information på nätet. Det blir för företagsledningen oundvikligen en fråga om varumärket. ”Skadas det eller stärks det av att vi blockerar det ena eller andra obehagliga materialet på Internet?” Och för det tredje kan operatörerna frestas eller tvingas att ge efter för filtreringskrav när de förhandlar med så kallade innehållsleverantörer. Den internationella mediekoncern som har rättigheterna till stora mängder film/teveprogram/musik med mera kan säga till operatören:

– Visst, ni får distribuera vårt material till era kunder, men bara om ni filtrerar bort sådant vi tycker stör våra affärer…

Guiden är indelad i fyra kapitel. I det första beskrivs vad filtrering egentligen innebär, i praktiska snarare än tekniska termer. I andra kapitlet behandlas frågan ”Vad ska filtreras?”. Vad anses i olika delar av världen acceptabelt respektive oacceptabelt och i vilken utsträckning används idag filtrering för att bli av med det oacceptabla? Tredje kapitlet fokuserar på juridiken. I vilken utsträckning kan operatörerna, den svenska riksdagen, EU eller Europadomstolen besluta om den typ av censur som filtrering innebär? I ett fjärde kapitel knyts resonemangen ihop med några avslutande reflektioner.

18 maj
22.25

18 maj
22.25



Vad menas med filtrering?

Kapitlet beskriver vad filtrering egentligen innebär rent praktiskt.

Föreställningen om webben (World Wide Webb) som en sfär där information ”ligger” för att bli ”tittad på” är inte alldeles felaktig, men den är starkt förenklad. Här är inte platsen att beskriva Internets många och intrikata funktioner, men själva interaktiviteten behöver särskilt betonas. Ofta sker i praktiken ett dolt, automatiserat informationsutbyte mellan den som vill ”titta” (A) och den som ”visar upp” information (B). B tittar många gånger in i A:s dator, kan man säga, innan B bestämmer vad som ska visas upp för A. B:s motiv för att göra så kan vara av olika slag. I ett fall kan B vilja kontrollera om A har behörighet att komma åt uppgifter som inte hålls tillgängliga för alla. I ett annat fall kan B vilja veta något om A:s intressen i syfte att lägga in annonser som passar A:s profil. (Vad har funnits på de webbsidor som A besökt tidigare – bilar? porr? klassisk musik?) I ett tredje fall kan B helt enkelt anpassa språket på sin webbplats efter det land A kommer från. I ett fjärde kan B vara ute i ärenden som är fientliga i någon mening – som att försöka placera skadlig eller åtminstone ovälkommen programkod hos A.

Det är alltså inte säkert att jag får se samma saker på min bildskärm som grannen får på sin, även om vi vid samma tillfälle besöker samma adress på Internet. Vad menas i en sådan miljö med ”filtrering”?

Någon allmänt accepterad definition av termen finns inte. I denna guide är filtrering avgränsad till att *en aktör med tekniska metoder försöker blockera flöden av specifik information som en annan aktör tillgängliggör för alla eller kommunicerar till några via Internet*.

Genom att skriva ”blockera” istället för ”försvåra” eller ”söka hindra” har författaren valt bort ett antal andra censurliknande, men mindre effektiva åtgärder för att begränsa informationsflöden på

nätet. Argumenten för sådana åtgärder är ofta desamma som för filtrering. Ett exempel är de som kan vidtas med hjälp av sökmotorn. En sökmotor (Google, Altavista, Yahoo med flera) är programmerad att rangordna sina träffar enligt vissa principer. Även om grundidén är att webbsidor ska rangordnas efter popularitet – till exempel så att sidor som får många besökare kommer högre upp på listan över träffar – tillåts också andra faktorer påverka rangordnandet. Hur sökmotorn ska ordna sina träffar är inte givet, och utom synhåll för de flesta Internetanvändare pågår hela tiden en kraftmätning mellan de ansvariga för sökmotorerna och alla de företag/intressen som slåss om förstaplatsen i sökmotorns kösystem. Av uppenbara skäl är det viktigt för till exempel företag som säljer tjänster eller varor att komma överst bland träffarna när användare av den för närvarande mest populära sökmotorn Google söker efter just deras typ av tjänst eller vara. Om de kan lista ut hur Google gör för att rangordna kan de utforma sin webbplats – och marknadsföring av den – så att den blir högre prioriterad. Google å andra sidan, ska för sin trovärdighet försöka upprätthålla vissa principer för vad som är rimligt och rättvist i rangordnandet av träffar.

Sökmotorns konstruktion betyder alltså mycket för vilken information användarna faktiskt hittar på nätet. I västvärlden, inte minst i USA, anser en stor majoritet av befolkningen att barn behöver skyddas från nakenhet, särskilt pornografi, varför Google har utvecklat en specialinställning kallad SafeSearch som innebär att träffar med nakenbilder utesluts. När barnen använder datorn ska de inte få hjälp med att hitta sådant ”vuxenmaterial”. Det barn som redan har adressen till en webbplats med nakenbilder kan skriva in den i webbläsarens adressfält och därmed finna det han/hon söker, men kan inte finna fler sådana adresser med sökmotorns hjälp.

2005 enades företagen bakom de största sökmotorerna i Tyskland (Google, Lycos Europe, MSN Deutschland, AOL Deutschland, Yahoo, T-Online, och t-info) att på detta sätt utesluta material som är ”skadligt för minderåriga”.[7]

Möjligheterna att med sökmotorernas hjälp försvåra för Internet-

7 Se: http://blogs.law.harvard.edu/ugasser/2005/06/10

användare att komma åt visst material ska inte diskuteras vidare här, men det är värt att nämna att Google, efter påtryckningar från Kina modifierade sin kinesiska version av sökmotorn så att landets filtreringssystem fungerade effektivare.[8]

Avsikten är nu inte att beskriva hur filtrering genomförs i teknisk mening. För den tekniskt kunnige är varken ”filtrering” eller ”blockering” några entydiga termer. De är snarare samlingsbegrepp för många olika åtgärder som, beroende på vilken sorts Internetanvändning det gäller – e-post, webbsurfning, peer-to-peer-kommunikation etcetera – syftar till att åstadkomma ett visst resultat.

”Först gäller det att identifiera det oönskade materialet … och därefter blockera det för Internets användare.”

Här räcker det att konstatera att filtrering rent praktiskt sker i två steg. Först gäller det att identifiera det oönskade materialet – fortsättningsvis förkortat OM – och därefter blockera det för Internets användare. Proceduren kan gå till på tre olika sätt:

1. **Manuell**. Detta är idag den vanligaste metoden för filtrering av webb-innehåll hos Internetoperatörer i demokratiska stater. Människor upptäcker OM som kommuniceras med hjälp av Internet och rapporterar till en central instans med uppdrag att övervaka och eventuellt filtrera nätet. Dessa människor kan vara anställda på myndigheter med uppgift att begränsa OM på nätet, eller engagerade medborgare som till en informationscentral rapporterar att de upptäckt till exempel barnporrbilder. Den centrala instansen har sedan ansvar för att ett filter, vanligen beläget hos Internetoperatörerna, uppdateras. Filtret släpper då inte igenom material som har vissa avsändare eller som eftersöks via vissa domäner, URL:er eller IP-nummer.

2. **Automatisk**. Datorprogram reagerar på visst OM (text, bilder, ljud) och blockerar det utan mänsklig inblandning. Primitiva tekniska lösningar kan bygga på identifiering av ”fula ord” i webbadresser, till exempel www.fuckingteenagers.com. Mer sofistikerade program ”undersöker” i någon mening det material som kommuniceras.

8 För detaljer om utvecklingen i Kina, se http://opennet.net/blog/2009/06/oni-releases-reports-filtering-asia-china.

Till de tekniskt ledande företagen på området hör NetClean Technologies i Göteborg. 2005 lanserade NetClean ett program avsett att installeras i servrar i lokala nätverk, till exempel hos organisationer eller företag. Det ”känner igen” många – men inte alla – barnporrbilder och slår larm när någon i det lokala nätet handskas med en sådan bild.
”NetClean ProActive är en unik mjukvara som blockerar åtgång till barnpornografiska bilder. NetClean samarbetar med polismyndigheter som klassificerar barnpornografiska bilder vilka NetClean ProActive sedan stoppar. Genom att jämföra mot existerande bilder kan NetClean ProActive stoppa bilden eller filmen till skillnad mot traditionella webbfilter som blockerar otillåtna adresser.”[9]
Även om det finns för polisen okända barnporrbilder som cirkulerar på Internet räknar användarna av NetCleans program med att det har en starkt avskräckande effekt. Få lär ta risken att befatta sig med barnporr på sin arbetsplats när risken för upptäckt är så stor.
2008 inledde NetClean samarbete med Teliasonera International Carrier, det företag i Teliasonera-koncernen som äger och hyr ut kapacitet i fibernät utanför Sverige. Internetoperatörer i Europa som betalar för att använda TIC:s nät kan kostnadsfritt få sin Internettrafik filtrerad med hjälp av ett annat av NetCleans program.[10] Här förekommer dock inget automatiserat sökande efter bilder. Filtreringen utgår från en svart lista på 800–1 000 webbadresser och uppdateras enligt TeliaSonera två gånger om dagen.[11] Vilka kunder som nappat på erbjudandet vill TIC inte avslöja. Rent teoretiskt, om alla kunder tackade Ja, skulle 85 procent av Internettrafiken i Europa komma att filtreras på detta sätt.

3. **En kombination av automatisk och manuell**. Ett datorprogram reagerar på visst OM men blockerar det inte utan vidarebe-

9 Citerat i november 2009 från NetClean Technologies webbsida: http://www.netclean.com/products.aspx?subPage=3

10 http://www.idg.se/2.1085/1.177542

11 Uppgift från en TeliaSonera-anställd med insyn i verksamheten, november 2009.

fordrar det till människor som granskar och fattar besluten. Man kan jämföra med den så kallade signalspaning som FRA numera sysslar med, eller det beryktade Echelon-systemet för avlyssning av internationell tele- och datatrafik. (Det senare bygger på ett samarbete mellan underrättelseorgan i främst engelsktalande länder, med USA:s National Security Agency, NSA, i centrum.) Signalspanandet syftar till att upptäcka, inte att filtrera, men det problem som behöver lösas är detsamma – att så enkelt som möjligt identifiera så mycket eftersökt material som möjligt i mycket stora informationsflöden.

När OM har identifierats finns olika metoder för själva filtreringen. En tekniskt möjlig men omständlig och därför ovanlig metod går ut på att radera ”fula” eller ”farliga” ord eller specifika bilder, varvid nätanvändaren bara ser tomma rutor på vissa webbsidor eller e-postmeddelanden. En annan variant är att hela webbsidan eller hela e-postmeddelandet blockeras när OM har identifierats. Ytterligare, mer drastiska metoder är att på servernivå blockera all information från det IP-nummer där OM har upptäckts eller att stänga allt dataflöde i en viss port. (Olika typer av dataflöden – e-post, webb, fildelning, nyhetsgrupper på nätet med flera – går på Internet via olika så kallade portar.)[12] Sådana metoder är också de mest problematiska ur principiell synpunkt. Det kan räcka med att till exempel en enda nakenbild har upptäckts för att utlösa blockeringen och att därmed väldiga mängder ”tillåtet” material också censureras.

Det måste samtidigt upprepas att filtrering i denna guides mening aldrig kan bli hundraprocentigt effektiv. Tekniskt kunniga eller mer drivna personer låter sig sällan stoppas av filter som har inrättats i avsikt att hejda information inom ett geografiskt område. Filter kan normalt kringgås till exempel av den som söker webbsidor med OM via en så kallad proxyserver belägen utanför området. OM kan spridas med fildelningsprogram, så kallad peer-to-peer, vilket gör det svårare att komma åt. Man kan tala om en kunskapsmässig kapprustning där båda parter hela tiden blir starkare. Den tekniska

12 Se: http://sv.wikipedia.org/wiki/Port_(datorteknik)

”…metoderna förfinas och förbättras, samtidigt som allt fler … får allt bättre kunskaper om nätets möjligheter och funktioner – och därmed om hur filter kan kringgås.”

utvecklingen fortgår. Filtreringsmetoderna förfinas och förbättras, samtidigt som allt fler Internetanvändare får allt bättre kunskaper om nätets möjligheter och funktioner – och därmed om hur filter kan kringgås.

Filtrering ger alltså inte total informationskontroll men kan duga till att hålla majoriteten av Internetanvändarna borta från OM. Om majoriteten är 80, 90 eller 98 procent av användarna beror på faktorer som varierar från fall till fall.

Till sist bör också nämnas möjligheten att blockera webbplatser genom överbelastning, så kallade DoS-attacker. En sådan attack innebär att en stor mängd anrop skickas fortlöpande från många datorer till en webbplats, ett datorsystem eller nätverk. Mottagaren blir därmed överbelastad så att övrig kommunikation kraftigt minskas eller upphör helt. Denna metod att knäcka, åtminstone tillfälligt, en webbplats har många gånger använts av enskilda aktörer i syfte att skada en politisk motståndare eller en konkurrent på marknaden.

I samband med den uppmärksammade kontroversen i Estland 2007 kring flyttandet av ett sovjetiskt-ryskt krigsmonument illustrerades hur sårbart ett litet lands Internetdrift kan vara. Flytten upprörde inte bara ester av rysk härkomst utan också många ryssar i Ryssland. Estlands regering, landets största bank och webbplatserna för flera större tidningar bombarderades med e-post och utsattes för så omfattande intrångsförsök att deras verksamhet på Internet lamslogs. Endast sedan man i Estland under några dagar hade blockerat all Internettrafik från utlandet kunde driften småningom återupptas.[13]

Inget hindrar dock statliga aktörer från att göra likadant. När ONI-forskarna studerade filtrering i Kirgizistan inför valet där 2005 fann de att större DoS-attacker genomfördes mot Internetoperatörer som hyste webbplatserna för två av oppositionens största tidningar. Forskarna kunde konstatera att attackerna utfördes av professionella hackers i Ukraina, men huruvida uppdraget kom från

13 Se: http://www.freedomhouse.org/template.cfm?page=384&key=206&parent=19&report=79#_ftnref16

politiska ledare i Kirgizistan eller från annat håll kunde aldrig utredas.

Vad kan filtreras?

En förteckning över vilket material man i olika delar av världen önskar filtrera blir lång. Nedan diskuteras olika kategorier av OM och vilka möjligheterna är till automatisk identifiering. Beslutsfattare som har planer på att mer ambitiöst rensa Internet på OM måste söka lösningar som antingen bygger på en grov/förenklad utsortering av OM, och som därmed sveper med åtskillig information som egentligen är ”godkänd”, eller som innefattar en hög grad av automatisering. Fortlöpande manuell granskning av Internetinnehåll för att urskilja det som bör filtreras är resurskrävande och sällan riktigt verkningsfull.

”Beslutsfattare … måste söka lösningar som antingen bygger på en grov/förenklad utsortering av OM, …, eller som innefattar en hög grad av automatisering.”

Det Internetinnehåll som idag filtreras i flest demokratiska stater är barnpornografi, och på operatörsnivå sker det alltid manuellt. Någon instans sammanställer svarta listor över webbadresser med barnporr som operatörerna sedan blockerar. Trots att barnporr i flera länder är det enda som filtreras, och trots att det är fråga om ett särdeles stötande material som allmänheten gärna hjälper till att bekämpa (det vill säga tipsa polis eller barnrättsorganisationer om när man stöter på det) är det svårt att manuellt göra filtren effektiva.

Vid läsning av nedanstående förteckning bör man minnas att inte ens Internetoperatörers datorkraft är obegränsad. Att viss automatisk identifiering av OM är tekniskt möjlig i vissa, avgränsade, informationsmiljöer – i forskningssammanhang eller på ett företags intranät – betyder inte att den är möjlig på Internetoperatörens nivå. Att hos operatören köra all Internettrafik genom till exempel ett program för identifiering av vissa bilder skulle bromsa nätets flöden alldeles för mycket. Här kan den framtida tekniska utvecklingen få stor betydelse för möjligheterna att filtrera. Den dag all Internettrafik kan köras genom avancerade program för identifiering av OM har förutsättningarna ändrats.

Med utgångspunkt från vilka krav på bekämpning av OM som i

olika sammanhang har ställts, kan alltså följande uppdelning göras:

- **Åsikter i text**. Det kan i totalitära stater vara regimkritisk argumentering vilken som helst, men det förekommer också i Europa. Franska och tyska domstolar har vid olika tillfällen krävt att de ansvariga för webbsidor blockerar pro-nazistisk propaganda och nazistiska symboler så att materialet inte görs tillgängligt inom domstolarnas jurisdiktionsområde. Att filtrera åsikter automatiskt är naturligtvis svårt. Datorprogram som med åtminstone något mått av träffsäkerhet kan skilja argumenterande text från faktapåstående text är inte science fiction, men även om det finns teorier om hur de skulle utformas återstår mycket arbete innan de kan fylla en praktisk funktion. Den dag det finns fungerande automatiska åsiktskontroller utvecklade för Internet är ännu långt borta.
  Handlar det om i förväg kända alster är filtrering rent tekniskt enklare. Antingen det gäller *Mein Kampf* i Tyskland eller Salman Rushdies roman *Satansverserna* i Iran är automatisk identifiering av verken en enkel sak. Några uppgifter om att sådan filtrering förekommer i praktiken har jag dock inte stött på.

- **Faktapåståenden i text**. I totalitära stater kan mycket vara OM, i Europa kan det gälla till exempel påståenden om att Förintelsen eller andra folkrättsbrott aldrig har ägt rum.

- **Bilder**. När det handlar om i förväg kända bilder finns datorprogram utvecklade för automatisk identifiering. De programmen kan också ”känna igen” bilder som har förändrats – till exempel beskurits, spegelvänts eller manipulerats färgmässigt – men bara till en viss gräns. En person som hyggligt väl behärskar program för bildbehandling kan lura system för automatisk identifiering. Gäller det bilder som inte är kända i förväg blir problemen och lösningarna annorlunda. Pornografi och annan nakenhet anstränger man sig i stora delar av världen för att filtrera bort. I USA och delar av Europa blockerar man i olika sammanhang sådant material för barn och ungdom, medan avsikten i bland annat Kina och många muslimska länder är att blockera det för

alla. Program för automatisk identifiering av nakenhet har hygglig träffsäkerhet men inte mer. De ”känner igen” bilder med mycket hudfärg och könsorganens typiska konturer, men kan därmed också komma att reagera för till exempel bilder från badstranden samtidigt som de missar många ”udda” sexbilder.
Om toleransen för heterosexuell mainstream-pornografi i många länder är liten brukar den vara ännu mindre för sexuella minoriteters pornografi.

- **Filmer**. Här gäller i allt väsentligt detsamma som för bilder. Stora medieföretag som BBC och CNN använder program för automatisk igenkänning av ansikten, röster och namnskyltar för att snabbt hitta i sina mycket stora filmarkiv. Vid automatisk sökning i gammalt filmmaterial används vanligen program som utnyttjar både filmbilderna och ljudet samtidigt.
Det är svårare att automatiskt identifiera nakenhet och sexaktiviteter på rörliga bilder än på stillbild, men det är inte omöjligt att nå hygglig träffsäkerhet även här.

- **Ljud**. Den öppna forskning och utveckling som sker inom området Spoken Document Retrieval, SDR, har praktiskt taget aldrig filtrering – i denna guides mening – som mål. (Här finns också åtskillig hemlig forskning, och vilka mål den har är obekant.) I takt med att de tekniska problemen med att automatiskt identifiera ljud löses ökar dock möjligheterna att filtrera, och argumenten för att filtrera ljud är inte svagare än för att filtrera text. Även här måste en indelning i kategorier göras.
En kategori ljud är ord, uttryck eller meningar, oavsett vem som talar. (På fackspråk *taligenkänning*.) Det är visserligen svårare att automatiskt känna igen talade ord än skrivna, men ändå förhållandevis lätt. De svårigheter som uppstår beror vanligen på att ljudkvaliteten är dålig eller ojämn, på störande bakgrundsljud, dialektala skillnader, inkorrekt grammatik, ordändelser som ”sväljs” med mera. Taligenkänning utnyttjas också i system för stöd åt funktionshindrade. Avsikten är att de med rösten ska kunna styra robotar eller andra tekniska system, till exempel i en specialanpassad lägenhet.

En annan kategori är *talarigenkänning*, det vill säga att automatiskt identifiera den talande personen. Här finns också system i praktisk tillämpning, till exempel för inpasseringskontroller. Detta kallas *talarverifiering*. För att en dörr ska öppnas måste personen X, som systemet har lärt sig känna igen, säga något i en mikrofon. System för talarigenkänning är förhållandevis dyra därför att de måste ”läras upp”. De är baserade på modeller för sannolikhetsteori, och för att datorprogrammen ska bli bättre fordras mycket övningsmaterial, det vill säga mycket inspelat tal av den person som ska kännas igen. Att ha god kontroll över ljudmiljön är avgörande för att bygga system som med stor träffsäkerhet känner igen enskilda individers röster.

En polisiär önskedröm vore att i de internationella tele- och datanäten ha spionprogram som ”känner igen” terroristers eller andra eftersökta personers röster. I en sådan dröm skulle, så fort till exempel Usama bin Laden sade något i en telefonlur, programmet slå larm och telefonens geografiska position bestämmas. Detta bygger på en vida spridd vanföreställning om att man ur varje inspelning av en mänsklig röst kan analysera fram ett unikt mönster, jämförbart med ett fingeravtryck, som med hygglig träffsäkerhet identifierar individen. Önskedrömmen kommer dock inte, åtminstone inte inom överskådlig tid, att infrias.[14]

För det första vore det i praktiken omöjligt att få in spionprogram i alla nät, för det andra saknar man vanligen det rikliga ljudmaterial som krävs för att kunna ”träna” programmen, och för det tredje har man inte – när ljudmaterial trots allt finns – tillräcklig kontroll över ljudmiljön för att ”träningen” ska fungera. Även om spionprogrammen kunde placeras ut i telenäten, och även om man som i bin Ladens fall har tillräckligt många ljudinspelningar av hygglig kvalitet kommer programmen inte att känna igen rösten förmedlad på en knastrig ledning från en telefonkiosk i norra Pakistan. Tilläggas kan också att de anhängare till bin Laden som utför själva terrordåden, och som därför kanske är viktigast att lokalisera, sällan är kända personer. Även

14 Se http://www.isca-speech.org/archive/eurospeech_2003/e03_0033.html

i de fall polis och säkerhetstjänster tror sig känna till deras identitet finns inte de ljudinspelningar som behövs för att ”lära upp” spionprogram.
En tredje kategori är ljud av annat slag än människoröster. Polisen behöver ibland ta reda på, vilket kan ske med hjälp av bakgrundsljud, var en ljud- eller videoinspelning är gjord. Även här är kontrollen över ljudmiljön viktig för automatisk igenkänning. När ljudkvaliteten är hög kan datorprogram ”höra” bättre än människor, till exempel skilja på olika fåglar av samma art när de sjunger. När kvaliteten är dålig blir programmens ”hörsel” också dålig.

- **Upphovsrättsligt skyddat material – text, ljud eller film**. Att identifiera enstaka verk, till exempel texter eller bilder, är alltså tekniskt inget problem och därmed är filtrering i princip genomförbar. För att komma åt piratkopiering mer generellt skulle dock krävas samlad information om de verk som är skyddade. Sådan finns inte idag, och att på nationell nivå avslöja – för att *automatiskt* filtrera – upphovsrättsbrott vore ett enormt resurskrävande och därtill komplext projekt som såvitt bekant inte har diskuterats på allvar någonstans.

- **Datorprogram**. Här handlar det främst om virus och annan destruktiv programkod, men det finns också ett intresse av att kunna blockera andra program, till exempel sådana med vars hjälp kopieringsskydd kan knäckas. Att automatiskt blockera datorvirus – utan stor överblockering – är idag inte realistiskt. Även om man kan identifiera vissa egenskaper hos programkoden som är typiska för virus, kan samma egenskaper återfinnas också i vanlig (nyttig) programkod.

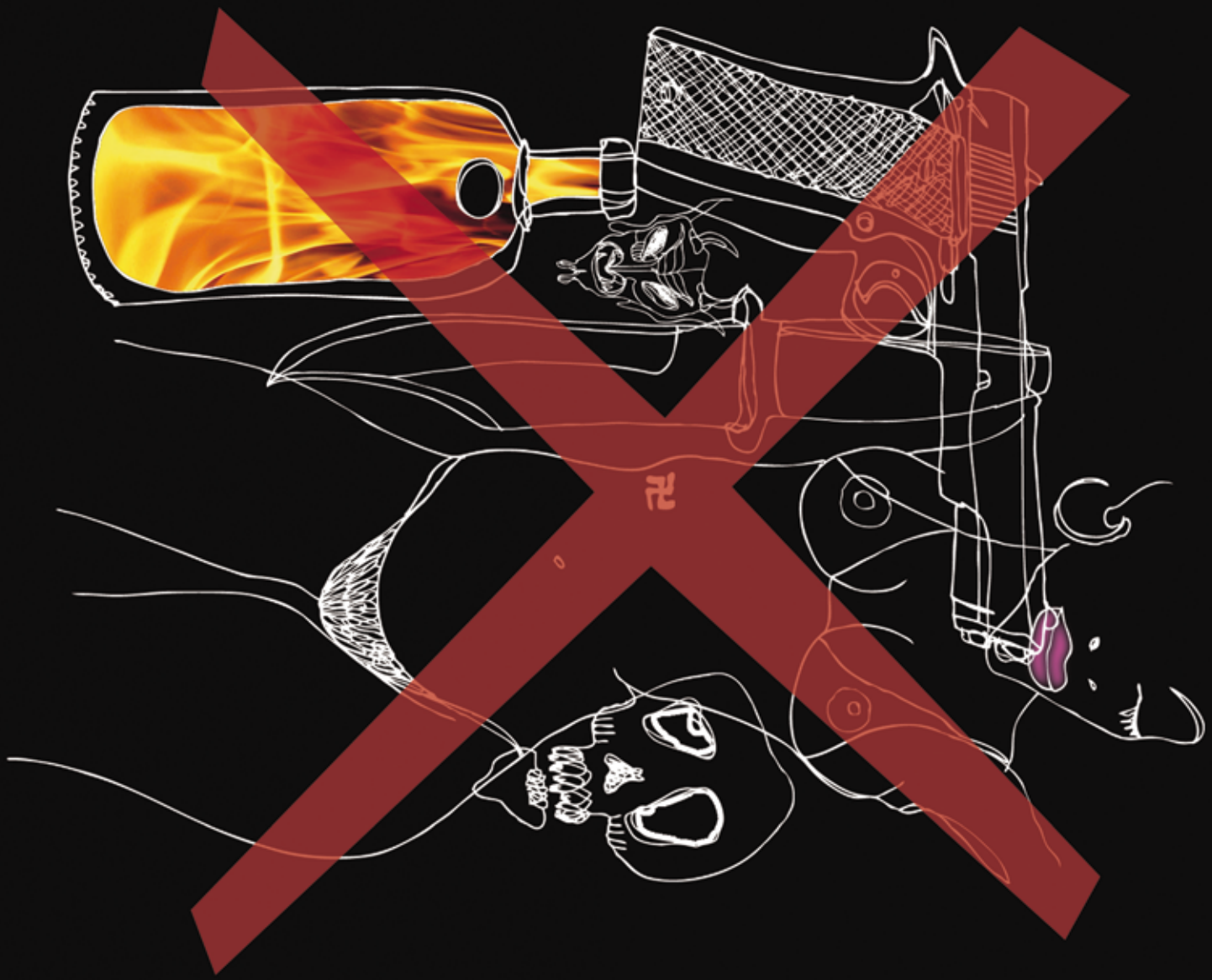
- **Skräppost filtreras rutinmässigt på många håll**. Internetoperatörerna kan med tämligen god träffsäkerhet upptäcka och filtrera sådan e-post. Anti-skräppost-program som automatiskt sorterar bort minst tre fjärdedelar – men ofta ännu mer – av all oönskad e-post i såväl servrar som slutanvändares datorer finns också att köpa. Programmen utgår vanligen från en uppsättning

regler med vars hjälp det kalkylerar sannolikheten för att det rör sig om skräppost. Förekomsten av stora bokstäver, utropstecken och vissa nyckelord (sex, porn, enlargement eller Viagra och liknande) är vanliga indikatorer. Även e-postbrevens struktur och layout vägs in. Eftersom problemet numera är så stort har många företag och andra större institutioner tekniska lösningar som innebär att all e-post körs genom skräppostfilter. (För svenska myndigheter, som i princip inte kan vägra att ta emot post, är situationen juridiskt besvärlig, men det är uppenbart att även de måste tillåtas använda sådana filter. Skräppost skulle annars ta stora delar av myndigheternas administrativa resurser i anspråk, vilket vore orimligt.)
Här pågår också en kunskapsmässig kapprustning. Skräppostproducenterna behöver komma förbi filtren och lär sig fortlöpande nya knep. Filtertillverkarna lär sig relativt snabbt att känna igen nya knep och täpper igen de hål som producenterna hittat. Kampen lär fortgå under överskådlig tid.

- **Phishing**, det vill säga bedrägerier som går ut på att lura Internetanvändare att lämna ifrån sig hemliga eller personliga uppgifter. I ett brev från något som ser ut att vara den egna banken uppmanas en kund att (för att ”förbättra säkerheten”, kanske) uppge kontonummer och personliga koder eller lösenord. Uppgifterna hamnar emellertid hos någon som bara är ute efter att stjäla pengarna på kontot – och som med hjälp koderna också kan göra det.
Phishing-brev är en form av skräppost som sällan kan fångas med filter. Som de flesta mer sofistikerade bedrägeriförsök kan de bara stoppas av den enskilde, det vill säga av det tilltänkta offret.

”Phishing-brev är en form av skräppost som sällan kan fångas med filter. Som de flesta mer sofistikerade bedrägeri-försök kan de bara stoppas av den enskilde, det vill säga av det tilltänkta offret.”

Illustration: © Camilla Laghammar



Vad är det onda som ska bort?

I det här kapitlet belyses frågan Vad ska filtreras? Vad anses acceptabelt och inte i olika delar av världen och i vilken utsträckning används filtrering idag för att bli av med det oacceptabla?

Krav på att statsmakten ska skydda medborgarna från OM, har förekommit så länge det funnits en fungerande statsmakt. (Med OM menas således allt som någon vill stoppa spridningen av.) Från det att tryckfriheten infördes i Sverige på 1700-talet och 200 år framåt var det främst blasfemi (hädelse), osedlighet (i modernt tal pornografi) och ärekränkning som stod i centrum. Upprördheten över hädandet ebbade dock ut och vid mitten av 1900-talet avskaffades förbudet helt. Vad pornografin beträffade inskränktes kraven på förbud under 1900-talets andra hälft till sådan som skildrade övergrepp på barn och – när det gällde vuxna aktörer/modeller – våldspornografi. Problem med ärekränkning och förtal lever vi fortfarande med.

Samtidigt har känsligheten ökat för andra uttryck i ord och bild. Förbudet mot det svensk lag kallar ”hets mot folkgrupp” skärptes väsentligt 1970 genom att definitionen av brottet vidgades från ”hets” till att omfatta även uttryck för ”missaktning” mot en folkgrupp. Det straffbara området utökades alltså så att det idag omfattar även lågmälda och mer resonerande yttranden som rymmer ”missaktning”. Även offentligt uppvisande av till exempel nazistiska symboler kan utgöra ”hets” i lagens mening. Vidare har de kategorier av människor som i hets-paragrafens mening utgör ”folkgrupper” utökats från fyra till fem. Tidigare var det förbjudet att uttrycka missaktning mot människor på grund av ras, hudfärg, nationellt/etniskt ursprung eller religiös övertygelse. Till detta lades 2003 sexuell läggning.

Reaktionerna mot högerextrem propaganda förefaller också att ha blivit starkare, liksom mot andra uttryck som uppfattas som

chockerande, hotfulla, sexistiska eller på annat sätt kränkande. Också vad gäller spridande av personuppgifter – inklusive uppgifter som alltid tidigare har betraktats som harmlösa – har känsligheten ökat.

Liknande skiftningar i vad som har ansetts vara OM återfinns i alla med Sverige jämförbara länder. Ledande politiker har ofta svårt att handskas med återkommande krav på statliga ingrepp mot OM. Å ena sidan lockas de av opinionsmässiga framgångar som kan följa av ingripanden mot företeelser som många medborgare finner stötande, å andra sidan är sådana ingripanden svåra att förena med de politiska ideal man normalt bygger sin politiska argumentation på – där yttrande- och informationsfrihet är centrala värden. Få politiker vill förknippas med censur eller åsiktsförbud.

Visst OM förbjuds helt enkelt i lag. De svenska grundlagarna rymmer för närvarande 18 yttrandefrihetsbrott. Därtill kan läggas ett 19:e – barnpornografi. Praktiskt taget all befattning med sådan pornografi är nu straffbar, men barnpornografin har ”lyfts ur” grundlagarna och räknas inte som yttrandefrihetsbrott utan som vanligt brott enligt brottsbalken. (Det vill säga polisiära ingripanden, åtal och rättegång sker på samma sätt som när det gäller misshandel, stöld och liknande.)

Utanför det grundlagsskyddade området är förbuden mot yttranden något fler och hantering med olika sorters information kriminaliserad i större utsträckning. (Se punkterna 2, 3, 4 och 7 i inledningens genomgång av lagstiftarens möjligheter att påverka Internetinnehåll.)

Därutöver har det länge ansetts acceptabelt att kontrollera, med olika metoder, medieinnehåll som är åtkomligt för barn och ungdomar. Det beslutas om åldersgränser för film, både på biografer och vid uthyrning. teveföretag beviljas sändningstillstånd där det bland annat stadgas att program som innehåller våld eller sex i vart fall inte ska sändas på tider då barn och ungdom normalt tittar. En statlig utredning föreslog 2009 inrättandet av en ny myndighet med uppgift att skydda barn och unga mot skadlig

mediepåverkan.[15] I skrivande stund (december 2009) är det oklart om förslaget kommer att realiseras.

Ytterligare ett exempel på den sortens riktade insatser mot OM är brottsbalkens förbud mot ”förledande av ungdom”. (Det återfinns i kap. 16 § 12.) Det brottsliga ligger här inte i yttrandens eller bilders innehåll utan i själva spridandet bland ungdom av sådant som pornografi eller propaganda för droger. En text som inom lagens ramar får säljas eller spridas i medier riktade till vuxna, får man alltså inte sprida vid till exempel en skola där den typiskt sett främst exponeras för barn eller ungdomar.

Till OM räknas naturligtvis också upphovsrättsligt skyddat material som sprids utan tillstånd.

ONI-projektet

Forskningsprojektet ONI (*Open Net Initiative*) påbörjades 2003 och har sedan dess avsatt en lång rad rapporter om filtrerandets omfattning och inriktning i olika länder. Ett omfattande material om projektet och dess resultat är tillgängligt via webbplatsen: http://www.opennetinitiative.net/.

ONI är ett samarbetsprojekt mellan fyra universitet: Harvard i USA, Toronto-universitetet i Kanada, samt Cambridge och Oxford i Storbritannien. Man har i huvudsak koncentrerat sig på att studera filtrering i diktaturer och auktoritärt styrda stater. Det är svårt av flera skäl. En del stater erkänner att filtrering pågår, andra inte. De som erkänner det lämnar sällan trovärdiga upplysningar om vad man undanhåller befolkningen eller hur man tekniskt och praktiskt går till väga.

Inom ONI har man därför tvingats utveckla en egen metod för att studera omfattningen av och effektiviteten hos olika regimers försök att filtrera. Man utgår från omfattande listor, som forskarna själva sammanställer, över potentiellt känsliga webbadresser. Via en

15 SOU 2009:51. Avskaffande av filmcensuren för vuxna, men förstärkt skydd för barn och unga mot skadlig mediepåverkan. http://www.sweden.gov.se/sb/d/11266/a/127925

så kallad proxyserver i det land som studeras undersöker man vilka av dessa webbadresser och sidor som kan nås inifrån landet.

När ONI 2008 sammanfattade fem års forskning i en bok[16] upprättade forskarna en förteckning över de kategorier av Internetinnehåll som någonstans i världen blockerats för användarna.[17] Det blev en lång lista över ämnesområden som delvis överlappar varandra men som sammantagna täcker stora delar av det innehåll och de tjänster som tillgängliggörs via Internet. Åtminstone någonstans i världen blockeras alltså material om:

1. Yttrande- och informationsfrihet
2. Politisk förändring och oppositionspartier
3. Politiska reformer, rättsliga reformer, regeringsarbetet
4. Militant opposition, extremister, separatister
5. Mänskliga rättigheter
6. Utrikespolitik och militära frågor
7. Minoriteters rättigheter och etniska frågor
8. Kvinnors rättigheter
9. Miljöfrågor

16 Deibert/Palfrey/Rohozinski/Zittrain. *Access Denied. The Practice and Policy of Global Internet Filtering.* (Tillträde förbjudet. Praktik och politik för världsomspännande Internetfiltrering.) The MIT Press 2008.

17 Av 40 undersökta länder fann ONI-forskarna att filtrering av Internet förekom i 24: Azerbadjan, Bahrain, Kina, Etiopien, Indien, Iran, Jordanien, Libyen, Marocko, Burma (Myanmar), Oman, Pakistan, Saudiarabien, Singapore, Sydkorea, Sudan, Syrien, Tadjikistan, Thailand, Tunisien, Förenade Arabemiraten, Uzbekistan, Vietnam och Yemen.
I två stater misstänkte man filtrering men hade av olika skäl svårt att belägga den: Vitryssland och Kazakstan.
I 14 av de undersökta länderna fann man inga tecken på filtrering: Afghanistan, Algeriet, Egypten, Irak, Israel, Kirgizistan, Malaysia, Moldavien, Nepal, Ryssland, Ukraina, Venezuela, Västbanken/Gaza och Zimbabwe. (Vad Ryssland beträffar omfattade studien dock bara ett urval Internetoperatörer baserade i Moskva.)
Det bör understrykas att filtrerandets omfattning i de studerade länderna varierar mycket.

10. Ekonomisk utveckling
11. Känslig eller kontroversiell historieskrivning, konst eller litteratur
12. *Hate speech* (ung: aggressiv hets mot folkgrupp)
13. Sexualkunskap och preventivmedel
14. Hälsofrågor
15. Homosexualitet
16. Pornografi
17. Utmanande klädsel
18. Kontaktsajter (*dating*)
19. Vadslagning och casinon
20. Spelsajter
21. Alkohol och droger
22. Minoriteters trosuppfattning
23. Religiös konvertering – kommentarer och kritik
24. Tjänster för anonymisering och för att kringgå teknisk spärrar
25. Hackning
26. Bloggtjänster och bloggdomäner
27. Webbhotel och webbportaler
28. IP-telefoni (*Voice over Internet Protocol*, VoIP)
29. Gratis e-posttjänster
30. Sökmotorer
31. Översättningstjänster
32. Multimedia-fildelning

33. P2P-kommunikation

34. Tjänster för gruppbildning och socialt nätverkande

35. Kommersiella webbplatser

ONI-forskarna urskiljer tre sorters ambitioner med filtrerandet i de totalitärt/auktoritärt styrda stater man studerat. För det första politik- och maktambitioner, för det andra sociala och moraliska ambitioner och för det tredje säkerhetsambitioner.

”Noteras kan att filtrering i syfte att skydda upphovsrätt inte finns med på listan.”

Noteras kan att filtrering i syfte att skydda upphovsrätt inte finns med på listan. I de stater som ONI hittills studerat betraktas den frågan uppenbarligen som mindre intressant, medan den i Europa och Nordamerika ständigt återkommer i diskussionerna om skärpt myndighetskontroll över Internet. I flera länder, bland annat Danmark, har man beslutat att den svenska webbplatsen Pirate Bay, känd/ökänd för att möjliggöra fildelning, ska blockeras.

Metoderna för att realisera filtrering av det oönskade materialet skiljer sig åtskilligt mellan de studerade länderna. Statliga organ, Internetoperatörer, webbhotell och/eller enskilda Internetcaféer kan där åläggas att utföra olika övervaknings- och blockeringsuppgifter.

Graden av sofistikation i filtrerandet varierar också. Åtskillig blockering är så primitiv att den bara bygger på nyckelord i webbadresser. Rymmer adresserna ord som *adult* eller *fuck* kan de hamna i filtret. Vanligast är att hela domäner blockeras, till exempel allt som ryms på: www.playboy.com, men det förekommer också att enskilda URL:er (adresser) under en domän väljs ut för blockering, till exempel www.playboy.com/girls/sex/features/sexy-girls-next-door-09/viewlarger7.html. I vissa länder blockeras alltid västliga nyhetssajter som BBC (www.bbc.co.uk/) och CNN (www.cnn.com/), medan nätanvändare i stater med en mer flexibel (och dyrare) filtreringsorganisation tillåts komma åt BBC och CNN de dagar inget ”olämpligt” rapporteras där.

Det är således av kostnadsskäl som de flesta länder väljer en tämligen grov eller primitiv form av filtrering. Att med mänskliga censorer aktivt övervaka informationsströmmarna på Internet i syfte att fortlöpande anpassa filtren blir oerhört resurskrävande. Av de

länder ONI har studerat är det endast Kina som mer uthålligt gör den sortens ansträngningar. Där är man också mer ”flexibel” och ”dynamisk” i sitt filtrerande än i något annat land.

Filtrering i parlamentariska demokratier

Det ställs i alla länder jämförbara med Sverige krav från olika samhälleliga aktörer på att OM på Internet ska kriminaliseras, bekämpas eller blockeras. Vanligen begär man nya lagregler eller mer effektiv tillämpning av redan existerande förbudslagstiftning, men kravställarna avstår många gånger från att precisera hur statsmakten borde gå till väga för att komma till rätta med OM-problem av olika slag.

Utgår man från kraven på/förslagen om bekämpande av olika sorters material – inte vad som faktiskt filtreras – kan som OM räknas:

- Barnpornografi
- Annan ”minoritetspornografi” (homosex, sadism/masochism med mera)
- Vanlig hetero-pornografi
- Nakenbilder/filmer utan pornografiskt syfte
- Prostitution
- Trafficking/människosmuggling
- Uppmuntran till homosexuella handlingar/homosexuellt umgänge
- Terrorism (att uppmana till, att berömma gärningsmän, att uttala stöd för…)
- Farlig kunskap, materiell: om vapen, bombtillverkning, gifter med mera
- Farlig kunskap, metoder: om hur man knäcker kopieringsskydd eller begår brott av annat slag, hur man begår självmord, annat destruktivt beteende

- Blasfemi, kränkning av något heligt – i praktiken av religiös tro eller religiösa symboler
- Rasism, *hate speech*, hets mot folkgrupp (inklusive förbud mot vissa symboler, till exempel nazistiska)
- Uppvigling (till brott)
- Förtal, ärekränkning (definierat på olika sätt)
- Lögner (främst vad gäller Förintelsen men också andra folkrättsbrott)
- Chockerande/makabert material (till exempel döda, lemlästade människor, filmade avrättningar, grovt underhållningsvåld)
- Illegalt spel (illegalt enligt nationell lag)
- Upphovsrättsligt skyddat material

Samlad kunskap om vad som faktiskt filtreras i länder vilkas styrelseskick påminner om Sveriges tycks inte stå att finna. En studie finansierad av The Open Society Institute, publicerad i oktober 2009, innehåller en ambitiös genomgång av de tekniska och juridiska aspekterna på filtrering i Europa och pekar på många exempel, men rymmer ingen sammanställning av uppgifter om det filtrerande som faktiskt pågår.[18] Pär Ström, med titeln Integritetsombudsman hos den borgerliga tankesmedjan Den Nya Välfärden, publicerade i januari 2009 en liten stridsskrift mot filtrering där han pekar på många exempel.[19] På engelska finns en rad böcker där författarna, med behovet av yttrandefrihet för ögonen, på samma sätt som Ström argumenterar mot filtrering. Från Wikipedia kan också åtskillig information hämtas, även om man under uppslagsordet ”Internetcensur” inte alltid håller isär

18 Callanan/Gercke/De Marco/Dries-Ziekenheiner: *Internet blocking – balancing cybercrime responses in democratic societies*. Aconite Internet Solutions 2009. http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf

19 Ström, Pär. *Storebror tar fram munkavlen. Internetfiltrering – censur som hotar yttrandefriheten*. Den Nya Välfärden, 2009.

filtrering på operatörsnivå från andra former av censurliknande åtgärder.[20]

"Det som skulle behövas är alltså fakta om vad som idag filtreras av olika Internetoperatörer i … länder med hyggligt fungerande demokratiska styrelseskick, …"

Det som skulle behövas är alltså fakta om vad som idag filtreras av olika Internetoperatörer i Europa, Nordamerika, Australien och andra länder med hyggligt fungerande demokratiska styrelseskick, och vilka beslut om ytterligare filtrering som har fattats av lagstiftande församlingar, domstolar eller Internetoperatörerna själva. Att samla in sådan kunskap kräver dock mer tid och resurser än författaren till denna guide förfogat över.

För att åtminstone komma en bit på vägen vände författaren sig i oktober 2009 till ETNO (European Telecommunications Network Operators' Association) för att få hjälp med en enkel enkätundersökning. ETNO är de europeiska telekomföretagens samarbetsorganisation. Enkäten innehöll bara fyra frågor: Filtrerar ert företag Internetinnehåll, utöver sådan filtrering som endast syftar till att tekniskt säkra driften av systemet, någonstans i Europa? Om svaret är Ja: I vilka länder filtreras vad? Vad motiverar filtreringen? Vilken metod används?

Företrädaren för ETNO förklarade sig inte beredd att lämna ut de e-postadresser till nyckelpersoner på medlemsföretagen som författaren skulle behöva för att själv göra enkäten. Däremot erbjöd hon sig att presentera enkäten för medlemmarna av en arbetsgrupp där en rad stora operatörer är representerade. Så skedde också. Jurister på ledningsnivå hos tretton av Europas största Internetoperatörer fick i början av november 2009 enkäten i sin hand. När denna guide går i tryck tre månader senare har inte ett enda svar inkommit.

Det säger inte något om huruvida operatörerna innehållsfiltrerar mycket eller lite, men det säger att de är medvetna om hur känslig frågan är.

Ett annat exempel på hur svårt det är att få information är arbetet med handelsavtalet ACTA, Anti-Counterfeiting Trade Agreement. Avsikten med dessa förhandlingar är att nå ett multilateralt avtal om bland annat metoder för att bekämpa upphovsrättsbrott. Stort hemlighetsmakeri omgärdar de diskussioner som förs. Del-

20 http://en.wikipedia.org/wiki/Internet_censorship

tagare är företrädare för bland andra EU, USA, Australien och Mexiko.

”Vissa uppgifter … tyder på att filtrering kan bli aktuell för att få bukt med spridningen av upphovsrättsligt skyddat material.”

Vissa uppgifter om innehållet i framlagda förslag har läckt ut från ACTA-förhandlingarna och tyder på att filtrering kan bli aktuell för att få bukt med spridningen av upphovsrättsligt skyddat material. Sådana uppgifter går dock inte att få bekräftade.[21]

Resterande del av detta kapitel ägnas en genomgång av länder och organisationer där filtrering beslutas eller diskuteras på hög politisk nivå. Den gör alltså inte anspråk på att vara heltäckande, utan är snarare en exempelsamling. Inte heller som sådan är den dock speciellt rättvisande. Särskilt svårt har det varit att få information om filtrering i före detta öststater som Polen, Tjeckien, Ungern, Bulgarien med flera. Flera personer engagerade i Internetfrågor i dessa länder uppger att de är tämligen säkra på att många Internetoperatörer filtrerar, åtminstone pornografi men möjligen också annat ”stötande” innehåll. Det går bara inte att få sådana uppgifter officiellt bekräftade.

Överhuvudtaget är skillnaderna i åsikter när det gäller acceptabelt respektive oacceptabelt i offentligheten betydande även inom Europa. 2009 har således Litauens parlament (Seimas) antagit en lag som ska skydda barn från material som rör homosexualitet, på samma sätt som de ska skyddas från information som skapar rädsla eller uppmuntrar till självstympning eller självmord.[22] Irländska parlamentets båda kamrar antog samma år en lag som förbjuder blasfemi, hädelse, samtidigt som många europeiska stater kraftfullt protesterade mot krav från ett antal muslimskt dominerade länder på liknande förbud. I vissa delar av Europa anses det nödvändigt att bekämpa nynazistiska strömningar genom att kriminalisera lögner, till exempel om massmorden på judar och romer under andra världskriget, medan man i andra delar (bland annat Sverige) anser att sådan lagstiftning snarare motverkar sitt syfte.

De flesta människor är födda och uppvuxna i en – bara en – social

21 http://arstechnica.com/tech-policy/news/2008/06/secret-acta-treaty-may-include-filtering-provisions.ars

22 http://list.amnesty.se/pipermail/pressnotiser/2009-June/000005.html

och rättslig kultur. Typiskt sett lever man sitt liv djupt nedsänkt i en föreställningsvärld där åtskilligt i form av historiska erfarenheter och värderingar är så självklart att man inte ens reflekterar över att det finns alternativ. Att förstå, på djupet, en annan föreställningsvärd, är mycket svårt. Utmaningen kan, som den amerikanske juristen Ronald J Krotoszynski skriver, jämföras med ”att be en fisk föreställa sig ett liv utan vatten”.[23] Att över kulturgränserna komma överens om gemensamma regler om yttrande- och informationsfrihet är en uppgift så svår att den gränsar till det omöjliga.

Internationella organisationer och filtrering

Europeiska Unionen, EU

Ambitionen att skydda unga mot OM har länge funnits inom EU, och det var därför fenomenet filtrering först hamnade på dagordningen. Det började med teve.

Inom dåvarande EG antogs 1989 ett direktiv med titeln ”Television utan gränser”[24] ett regelverk som har moderniserats i flera omgångar och som fortfarande utgör grunden för EU:s politik i tevefrågor. Två principer står i centrum: fri rörlighet för europeiska teveprogram på den inre marknaden och skyldighet för tv-kanalerna att reservera mer än hälften av sin sändningstid för europeiska verk, där så är praktiskt möjligt.

Direktivet ska dock också uppfylla vissa *”viktiga mål av intresse för allmänheten, till exempel kulturell mångfald, skydd av minderåriga och rätt till genmäle”* heter det i direktivets förord. Det anses *”nödvändigt att införa regler för program och tevereklam för att skydda minderårigas fysiska, mentala och moraliska utveckling.”*

I direktivets artikel 22 utvecklas detta:

”Medlemsstaterna skall vidta lämpliga åtgärder för att säkerställa att tevesändningar från teveprogramföretag inom respektive stats jurisdiktion inte

23 Krotoszynski, Ronald J. *The First Amendment in Crosscultural Perspective*. New York University Press 2009, sid 6.

24 89/552/EEG

inkluderar program som allvarligt kan skada den fysiska, mentala eller moraliska utvecklingen hos minderåriga, särskilt program som innehåller pornografi eller meningslöst våld."

I en rapport från EU-kommissionen till rådet 2001 om tillämpningen av Televisions-direktivet heter det bland annat: *"Barn tittar oftare ensamma på teve, och antalet tevekanaler har ökat så mycket att det är svårt för myndigheterna att övervaka dem. Genom digital teknik kan tittarna själva bestämma vid vilken tidpunkt de skall se olika program, och det är omöjligt att övervaka sändning via Internet.*

Den s.k. V-chiptekniken som används i Nordamerika är tekniskt olämplig i Europa. Denna teknik håller dessutom på att bli förlegad, eftersom den grundas på analog teknik. Digitala sändningar ger mycket mer sofistikerade och tillförlitliga möjligheter att filtrera och spärra olämpliga program. Teknisk utrustning kan aldrig helt ersätta programföretagens ansvar.

Set-topboxar och digitala teveapparater skall vara driftskompatibla så att olika programvaror för att filtrera och spärra program kan installeras på samtliga. Ett harmoniserat bedömningssystem är omöjligt pga. kulturella skillnader, men genom digital teknik kan man få filtersystemen att fungera på ett flexibelt och kulturellt anpassat sätt."[25]

2007 beslutade EU om ett direktiv[26] som med hänvisning till nya tekniker för tevesändningar ändrar vissa delar av det gamla Televisionsdirektivet. I de inledande motiveringarna till 2007 års beslut heter det på punkt 45:

"De åtgärder som vidtas för att skydda den fysiska, mentala och moraliska utvecklingen för minderåriga och den mänskliga värdigheten bör noga vägas mot den grundläggande yttrandefriheten, såsom den slås fast i Europeiska unionens stadga om de grundläggande rättigheterna. Syftet med dessa åtgärder, såsom användning av personliga identifieringsnummer (PIN-koder), filtersystem eller märkning, bör därmed vara att garantera en tillfredsställande nivå på skyddet för den fysiska, mentala och moraliska utvecklingen för minderåriga och mänsklig värdighet, särskilt när det gäller audiovisuella medietjänster på begäran."

Utvecklingen inom teveområdet innebär bland annat att teve-

25 KOM/2001/0009

26 2007/65/EG

sändningar i åtminstone ett avseende kan förmedlas enligt villkor som gäller för Internet: tjänster skapas genom vilka man kan titta på vilket program som helst när som helst på dygnet. När en svensk utredning om en ny radio- och tevelag föreslog nya regler om sådan så kallad beställteve konstaterade den bara att EU kräver att barn och unga ska skyddas mot verklighetstrogna våldsskildringar och pornografi, och att filtrering har angetts som ett alternativ för att nå det målet.[27]

Sammanfattningsvis har EU alltså inte ställt uttryckliga krav på filtrering av teveprogram, men har heller inte släppt tanken.

"Sammanfattningsvis har EU alltså inte ställt uttryckliga krav på filtrering av teveprogram, men har heller inte släppt tanken."

När Internet började bli allmänt tillgängligt i Europa vid slutet av 1990-talet initierade EU tidigt ett *Safer Internet*-program. Det syftar i första hand – men inte enbart, målformuleringarna är bitvis vaga – till att skydda minderåriga.

Safer Internet Programme är ett löpande projekt som för närvarande arbetar med en femårsbudget på 45 miljoner euro – drygt 450 miljoner kronor. Ett av flera mål är att utveckla möjligheter till filtrering via innehållsmärkning enligt så kallade Rating Systems. Om till exempel alla webbsidor kategoriserades enligt en enkel mall skulle ju filtrering underlättas oavsett på vilken nivå man ville utföra den. På sin egen webbplats beskriver 2009 de ansvariga för Safer Internet målet (i min översättning).

"För att kunna bekämpa spridningen av illegalt material på Internet finansierar The Safer Internet Programme projekt som syftar till att höja effektiviteten hos existerande datorprogram för filtrering och övervakning, liksom projekt för att utveckla nya metoder för innehållsmärkning."[28]

Försöken att skapa bred internationell uppslutning bakom ett system för innehållsmärkning kanaliserade EU först till Internet Content Rating Association, ICRA, som skapat både ett system för märkning av webbsidor och filter anpassade till systemet. 2009 går ett liknande projekt under namnet Quatro Plus.[29] Hittills tycks

27 SOU 2008:116

28 http://ec.europa.eu/information_society/activities/sip/projects/filter_label/index_en.htm

29 http://ec.europa.eu/information_society/apps/projects/factsheet/index.cfm?project_ref=SIP-2006-UE-211001

dock ingen av EU:s satsningar på innehållsmärkning ha fått något större genomslag.

Allmänt hållna önskemål om filtrering – nästan alltid med reservationer för att intresset av yttrandefrihet måste beaktas – återkommer i många EU-dokument. I en ”rekommendation” från ministerrådet och EU-kommissionen 2006 heter det bland annat att *”industrin för audiovisuella tjänster och nätverksbaserade informationstjänster liksom andra berörda parter”* bör *”undersöka möjligheten att skapa filter som förhindrar att information som kränker människans värdighet sprids på Internet”*.[30]

”… stödja utbyggnaden … av den sorts barnporrfilter som används i bland annat Sverige, … genom svartlistning av webbplatser där man funnit barnpornografi publicerad med kommersiellt ändamål.”

I februari 2008 beslöt EU-kommissionen att stödja utbyggnaden i medlemsländerna av den sorts barnporrfilter som används i bland annat Sverige, det vill säga genom svartlistning av webbplatser där man funnit barnpornografi publicerad med kommersiellt ändamål. EU anslog 550 000 euro (cirka 5,5 miljoner kronor) för ändamålet.[31]

Också i kampen mot terrorism har EU aktualiserat filtrering. Franco Frattini, fram till 2008 vice ordförande i EU-kommissionen och med ansvar för rättsliga frågor, ville använda filtrering som redskap i kampen mot terrorismen.

–Jag tänker låta undersöka hur det kan vara möjligt att hindra människor från att använda eller söka farliga ord som ”bomb”, ”döda”, ”folkmord” och ”terrorism”, sa han i ett tal i Europaparlamentet 2007-09-05.[32] På sin officiella webbplats förklarade han 2007-09-14 att det borde vara möjligt att blockera till exempel webbsidor med information om hur man tillverkar bomber.[33]

När ministerrådet den 28 november 2008 beslöt om ändringar i rambeslutet från 2002 om bekämpande av terrorism, ställde man

30 Rättelse till Europaparlamentets och rådets rekommendation 2006/952/EG av den 20 december 2006 om skyddet av minderåriga och människans värdighet och om rätten till genmäle med avseende på konkurrenskraften hos den europeiska industrin för audiovisuella tjänster och nätverksbaserade informationstjänster. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:156:0038:0043:SV:PDF

31 http://www.sr.se/ekot/artikel.asp?artikel=1883339

32 http://www.dn.se/nyheter/varlden/eu-topp-vill-forbjuda-terrorord-1.730818

33 Se bland annat Frattinis kommentar den 14 september 2007 på: http://ec.europa.eu/commission_barroso/frattini/news/archives_2007_en.htm#september

krav på medlemsstaterna att kriminalisera bland annat ”utbildning för terroristsyften”, med vilket menas:

”att tillhandahålla instruktioner för tillverkning eller användning av sprängämnen, skjutvapen, andra vapen eller skadliga eller farliga ämnen, eller instruktioner om andra speciella metoder eller tekniker, i syfte att begå något av de brott som anges i artikel 1.1 a–h och med vetskap om att de kunskaper som tillhandahålls är avsedda för detta ändamål.”[34]

Däremot sades i beslutet 2008 ingenting uttryckligt om filtrering eller blockering av Internetinnehåll. Frattinis sätt att få stopp på ”terroriststödjande” information realiserades inte – åtminstone inte denna gång.

EU:s så kallade Stockholmsprogram, som bland annat handlar om brottsbekämpning inom unionen, antogs i december 2009.[35] Där heter det (egen översättning):

”Bekämpandet av barnpornografi på Internet fordrar nära samarbete med den privata sektorn för att identifiera och stänga ned eller blockera tillgång till webbplatser med innehåll avsett för pedofiler, vilket dock måste ske på ett formellt korrekt sätt. Europol måste här få spela en central roll genom att utveckla en plattform för identifiering av de webbplatser på nätet som innehåller barnpornografi, och därmed möjliggöra ett effektivt samarbete medlemsstaterna emellan.”

Här talas alltså om filtrering endast i samband med barnpornografi. Formuleringar i tidigare versioner av Stockholmsprogrammet tydde på att man tänkte sig filtrering som ett alternativ även i andra sammanhang, men i slutdokumentet är detta borta.

Det är svårt att tolka EU:s beslut och rekommendationer på annat sätt än att uppfattningarna om filtrering går isär inom unionen. Möjligheten att blockera material för Internetanvändarna dyker

34 RÅDETS RAMBESLUT 2008/919/RIF av den 28 november 2008 om ändring av rambeslut 2002/475/RIF om bekämpande av terrorism. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008F0919:SV:HTML

35 Stockholmsprogrammet ska, som den svenska regeringen beskriver det på sin webbplats, ”ange ramarna när det gäller EU-arbetet för polis- och tullsamarbete, räddningstjänst, straffrättsligt och civilrättsligt samarbete, asyl, migration och viseringspolitik för åren 2010–2014.”
Den officiella beteckningen är COM (2009) 262. Texten återfinns på: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0262:FIN:EN:PDF

upp i många sammanhang, men med undantag för barnpornografin tycks man inte ha nått tillräcklig enighet för att kunna driva frågan mera kraftfullt. Några initiativ eller principiella ställningstaganden i syfte att förhindra eller begränsa Internetoperatörers egen filtrering inom EU tycks inte heller ha förekommit.

Europarådet

Europarådet grundades 1949 med uppgift att utveckla gemensamma demokratiska principer i Europa, i första hand med utgångspunkt från Europakonventionen om de mänskliga rättigheterna. Rådet har 47 medlemsstater. Några större länder utanför Europa, bland annat USA och Japan, deltar med observatörsstatus.

Rådet beslutade den 26 mars 2008 officiellt om en rekommendation till medlemsstaterna *"beträffande åtgärder för att markera respekten för yttrande- och informationsfriheterna i samband med användning av Internetfilter."*[36]

Rekommendationen inleds med en lång rad påpekanden om värdet av yttrande- och informationsfriheterna. Där erinrar Rådet också om en tidigare rekommendation (från 2001) som uppmuntrade till "innehållsmärkning" av webbsidor i syfte att underlätta för användarna att filtrera bort oönskade sidor.[37]

Därefter följer elva punkter som enligt Europarådet behöver beaktas när filtrering av Internet ändå företas. Här preciseras inte vem/vilka råden vänder sig till, men utgångspunkten tycks vara att filter är något som Internetanvändare (*users*) utsätts för av andra aktörer. Sannolikt är det i första hand Internetoperatörerna som förväntas ta till sig de elva punkterna, men även Internetcaféer, skolor och bibliotek kan höra till målgruppen. Råden är allmänt

36 Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters. https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2008)6&Language=lanEnglish&Ver=original&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75

37 Recommendation Rec(2006)12 of the Committee of Ministers to member states on empowering children in the new information and communications environment.

hållna och handlar om att användarna ska få kännedom om att filtrering sker och vilken teknik som används för den. De ansvariga för filtrering ska fortlöpande granska och uppdatera filtren, ska utbyta erfarenheter enligt modellen *best practices* med mera. Alla inblandade rekommenderas till ökad medvetenhet om fördelar och risker med filter.

Mot slutet påpekas att medlemsstaterna – och då talar man om de politiska beslutsfattarna – bara får använda filtrering av Internet på nationell nivå om villkoren i artikel 10, paragraf 2 i Europakonventionen är uppfyllda. Artikel 10 ska garantera yttrandefriheten. Den får inskränkas bara under former *"som är föreskrivna i lag och som i ett demokratiskt samhälle är nödvändiga med hänsyn till den nationella säkerheten, den territoriella integriteten eller den allmänna säkerheten, till förebyggande av oordning eller brott, till skydd för hälsa eller moral, till skydd för annans goda namn och rykte eller rättigheter, för att förhindra att förtroliga underrättelser sprids eller för att upprätthålla domstolarnas auktoritet och opartiskhet."*[38]

Sammanfattningsvis uppvisar Europarådet samma ambivalens inför Internetfiltrering som så många andra. ("Helst ingen filtrering, men om det är absolut nödvändigt så…") Närmare besked om när det kan vara absolut nödvändigt ges inte.

OSCE

Organisationen för säkerhet och samarbete i Europa (på engelska förkortat OSCE, på svenska OSSE) arbetar med bland annat konflikthantering och medborgerliga rättigheter i Europa. Den bildades under kalla kriget som ett forum för dialog mellan väst och öst och ingår sedan 1993 som en regional organisation inom FN. Fram till 1995 hette den Europeiska säkerhetskonferensen (ESK). Den har 56 medlemsstater, däribland flera icke-europeiska – bland andra USA och Kanada.

OSCE ägnar betydande energi åt att bevaka yttrande- och infor-

38 Europakonventionen på svenska återfinns på: http://www.echr.coe.int/NR/rdonlyres/1009F7DB-87E3-4056-8E17-8A8A41768BA7/0/SwedishSuédois.pdf

mationsfriheterna. Någon specifik satsning på filtreringsfrågor tycks inte ha förekommit, men i flera skrifter har organisationen uttalat sig kategoriskt i frågan om statens roll vid filtrering. 2005 heter det (egen översättning):

"I ett modernt demokratiskt och välfungerande samhälle bör medborgarna själva kunna bestämma vad de vill komma åt på Internet. Rätten att sprida och ta emot information är en grundläggande mänsklig rättighet. Statligt påbjudna mekanismer for filtrering, innehållsmärkning eller blockering av innehåll är inte acceptabla."[39]

2007 återkommer man till samma principiella ställningstagande (egen översättning):

"Regeringars beslut om blockering eller filtrering av innehåll på Internet strider mot OSCE:s normer. I ett demokratiskt och öppet samhälle är det medborgarnas/användarnas sak att bestämma vad de ska söka fram på Internet."[40]

Enskilda länder och filtrering

Australien

"Av skäl som för en utomstående betraktare inte är uppenbara har Australien i tio år varit särskilt aktivt vad gäller statlig, politiskt bestämd filtrering."

Av skäl som för en utomstående betraktare inte är uppenbara har Australien i tio år varit särskilt aktivt vad gäller statlig, politiskt bestämd filtrering. År 2000 lagstiftades om en skyldighet för landets Internetoperatörer att radera innehåll som bedömdes vara obehagligt eller skadligt (*disturbing or harmful*) för personer under 18 år.[41]

En mer ambitiös och därmed kontroversiell filtreringssatsning, "The Cyber-safety Plan", påbörjades 2007. På regeringens hemsida återfinns bland annat följande (egen översättning):

"Ett moment i den Australiensiska regeringens plan för cyber-säkerhet är introducerandet av filtrering på Internetoperatörsnivå. Det är regeringens

39 *The Media Freedom Internet Cookbook*. OSCE 2004. Sid 19.

40 *Countering Terrorism, Protecting Human Rights*. A manual. OSCE/ODIHR 2007. Sid 231. Kan laddas ned via: http://www.osce.org/odihr/item_11_28294.html

41 *A Starting Point: Legal Implications of Internet Filtering*. OpenNet Initiative, september 2004. Sid 4. http://opennet.net/docs/Legal_Implications.pdf

uppfattning att operatörerna bör ta ett visst ansvar för att möjliggöra blockering av "förbjudet" material på Internet, precis som de gör i ett antal andra utvecklade västländer.

Före valet lovade regeringen att initiera filtrering av innehåll med hjälp av en "svart lista" över förbjudna webbplatser, en lista som Australiens Kommunikations- och Medieverk (ACMA) upprättar enligt krav som fastställs i lag."[42]

Även om den australiensiska regeringen i sin information betonar att det huvudsakligen (*predominently*) är barnpornografi som filtrerandet ska skydda mot, uppgav den på direkt fråga vid en hearing i parlamentet i maj 2009 att mindre än en tredjedel av de svartlistade webbadresserna rymde barnpornografi. Exakt vad som döljer sig bakom de övriga två tredjedelarna har dock inte redovisats officiellt. Enligt webbplatsen www.couriermail.com.au den 29 oktober 2008 handlar det om vanlig pornografi, bestialitet, allvarligt våld med eller utan koppling till sex, detaljerade instruktioner om hur brott begås, hur våld utövas eller droger används, eller material som uppmanar till terrorism. (Begreppet bestialitet är något oklart i detta sammanhang. Engelskans *bestiality* kan syfta på tidelag, det vill säga sex mellan människa och djur, men också på råhet i största allmänhet.)[43]

Sedan 2008 har flera operatörer fortlöpande testat filtrering av webbadresser enligt svarta listor som den ansvariga myndigheten, ACMA, upprättat. Svårigheterna med projektet illustrerades – och det gav kritikerna vatten på kvarn – när en sådan lista med drygt 2 000 webbadresser läckte ut och visade sig rymma bland annat adressen till en tandläkare, en kennel och ett konsultföretag inriktat på att hjälpa cafeterior.[44] Trots den hårda kritiken mot projektet håller dock Australiens premiärminister Kevin Rudds regering fast vid målet: att alla landets Internetoperatörer ska vara skyldiga att filtrera de webbadresser som förekommer på den lista som den stat-

42 http://www.dbcde.gov.au/online_safety_and_security/cybersafety_plan/internet_service_provider_isp_filtering

43 http://www.news.com.au/couriermail/story/0,23739,24567413-8362,00.html

44 http://www.wikileaks.org/wiki/A_Blacklist_for_Websites_Backfires_in_Australia

liga myndigheten ACMA upprättar och fortlöpande uppdaterar. Vilka dessa webbadresser är ska vara hemligt.

Belgien

Operatören Scarlet Extended Ltd ålades 2007 av en belgisk domstol att stoppa olaglig fildelning bland kunderna. Motpart i målet var SABAM, en organisation för författare, publicister och kompositörer som hävdade att Scarlet medverkade till brott mot EU:s upphovsrättsdirektiv. Operatören fick sex månader på sig att installera en teknisk lösning med vars hjälp fildelningen kunde stoppas. Fanns tekniken inte på plats efter sex månader skulle företaget därefter betala vite med 2 500 euro per dag tills installationen var klar.[45]

Sedan det visat sig att ingen av de tekniska lösningar för filtrering som SABAM hänvisat till fungerade, hävdes 2008 domen vad gällde vitet.[46] Frågan om Scarlet kan anses medansvarigt för den illegala spridningen av upphovsrättsligt skyddat material ska dock prövas i högre instans. I skrivande stund (december 2009) föreligger ingen dom i målet.

Brasilien

Den brasilianska modellen och tevekändisen Daniela Cicarelli videofilmades 2006 när hon på en badstrand i Spanien ”utförde intima handlingar” med sin pojkvän Renato Malzoni. Filmen hamnade snart på Youtube och blev omåttligt populär. Paret Cicarelli/Malzoni hotade stämma Youtube om inte videosekvensen togs bort, och Youtube försökte verkligen. Problemet var bara att användarna envisades med att lägga in filmen på nytt.

En domstol beslöt att brasilianska Internetoperatörer skulle blockera videofilmen. Två större operatörer blockerade då hela Youtube. Efter en del förvirring och debatt i de rättsliga frågorna hävdes

45 Computer Sweden 2007-08-22. http://www.idg.se/2.1085/1.114347

46 Pressmeddelande 2008-10-24 från den Washington-baserade advokatbyrån Crowell & Moring. http://www.crowell.com/NewsEvents/PressRelease.aspx?id=229

blockeringen. Man försöker nu, efter förmåga, att blockera endast filmen med Cicarelli/Malzoni. Den har dock spridits till så många andra, mindre webbplatser för gratis videoklipp att ansträngningarna i praktiken har varit förgäves.[47]

I april 2008 fattade en domstol ett beslut av samma typ som i Cicarelli-fallet. Man krävde att operatörerna skulle blockera en blogg där skribenten (eventuellt) gjorde sig skyldig till förtal. Bloggen använde programvara från den stora bloggtjänsten Wordpress, men eftersom det var enklare att blockera hela Wordpressdomänen än en enskild blogg valde operatörerna den lösningen. Ett stort antal bloggar som inte berördes av domstolsbeslutet blockerades därmed.[48]

Upplysningar om vad som sedan hänt – i vilken utsträckning andra Wordpressbloggar fortfarande är blockerade i Brasilien – är svårt att finna.

Danmark

I Danmark började Internetoperatörerna 2005 blockera barnpornografi enligt samma modell som Sverige, det vill säga de gör det utan att vara tvingade genom lagstiftning.

I ett par fall har också domstolar beordrat operatörer att blockera utländska webbplatser med hänvisning till att de bidrar till spridning av upphovsrättsligt skyddat material: det gäller till exempel den ryska allofmp3.com (år 2006) och svenska The Pirate Bay (2008).[49]

”I ett par fall har också domstolar beordrat operatörer att blockera utländska webbplatser med hänvisning till att de bidrar till spridning av upphovsrättsligt skyddat material.”

Finland

Också i Finland filtreras barnpornografi, och precis som i Sverige förser polisen Internetoperatörerna med en svart lista över webb-

47 http://opennet.net/blog/2007/01/youtube-does-brazil

48 http://opennet.net/blog/2008/04/brazil-court-orders-isps-block-access-wordpress-blog

49 Ström, Pär. *Storebror tar fram munkavlen. Internetfiltrering – censur som hotar yttrandefriheten*. Den Nya Välfärden, 2009. Sid 22.

adresser. Blockerandet är frivilligt för operatörerna, men som en tydlig viljemarkering har den finska riksdagen stiftat en lag som ger operatörerna rätt att blockera just barnpornografi och polisen rätt att förse dem med svartlistade adresser. Lagen trädde i kraft 1 januari 2007.

Den stadgar också att listan över blockerade webbadresser ska hållas hemlig. Vid ett tillfälle läckte den emellertid ut, och filtreringsmotståndaren Matti Nikki publicerade den på sin webbplats för att – hävdade han själv – visa att det också fanns laglig (vuxen) pornografi på de webbplatser som blockerades. Resultatet blev att även Nikkis webbplats fördes upp på svarta listan.[50] Polis och åklagare utredde under ett år om Nikki skulle åtalas, men våren 2009 beslöt man lägga ner förundersökningen.[51]

Frankrike

I Frankrike har filtreringsfrågan aktualiserats i flera omgångar.

När antinazistiska aktivister år 2000 drog det amerikanska jätteföretaget Yahoo inför fransk domstol, avfärdades de först av företagets amerikanska jurister med en axelryckning. Målet handlade om en auktionstjänst hos Yahoo där nazistiska memorabilia bjöds ut. Där fanns armbindlar med svastika, dolkar och medaljer att köpa för högstbjudande. Alla världens Internetanvändare, även de franska, kunde se föremålen och delta i auktionen. De franska aktivisterna hävdade att hanteringen var olaglig i Frankrike och borde stoppas där.

Orimligt, hävdade Yahoo. Fransk lag må förbjuda alla nazistiska yttringar i Frankrike, även sådana här auktioner. Men franska domstolar kan inte besluta om vad ett amerikanskt företag får ha i sina servrar i USA!

Men de franska domstolarna formulerade inte saken på det sättet. De bedömde, efter att ha konsulterat tekniska experter, att Yahoo oftast kunde avgöra från vilket land en person loggade in till auktions-

50 Ström 2009, sid 23. Se också: http://www.idg.se/2.1085/1.146913

51 http://www.hbl.fi/text/inrikes/2009/3/10/w24548.php

tjänsten och att det därmed var tekniskt möjligt att sätta upp ett filter för just franska besökare. Företaget ålades därför att ”avskräcka och hindra” (*deter and prevent*) personer i Frankrike från att komma åt auktionstjänsten ifråga. En dom med den innebörden vann småningom laga kraft i Frankrike.[52]

Det rättsliga efterspelet blev utdraget, med rättegångar i både Frankrike och USA. Exakt hur Internetoperatörer i Frankrike idag gör för att efterleva domstolens order är oklart. Pär Ström uppger dock att sökmotorer som används i Frankrike ska vara försedda med nazi-filter, det vill säga de ska inte kunna användas för att söka efter webbadresser där det finns nazistiskt material.[53]

Under 2008–2009 har det pågått en hård strid i landet om de så kallade HADOPI- och LOPPSI 2-lagarna. HADOPI har i första hand kommit till för att stoppa illegal spridning av upphovsrättsligt skyddat material via Internet. Lagen var kontroversiell bland annat därför att regeringen ville skapa en möjlighet att stänga av användare från Internet genom ett administrativt beslut, det vill säga utan domstolsprövning. Just denna fråga var central när EU efter långa diskussioner enades om det så kallade Telekompaketet i november 2009. Huruvida medlemsländerna enligt paketet faktiskt är skyldiga att överlåta beslut om avstängning på domstol är dock fortfarande en öppen fråga. Den text man slutligen enades om ger inte klarhet. Nederländerna och Storbritannien förbereder lagar som liknar den franska.[54] Också Spanien har utpekats som ett land med HADOPI-planer, men här går uppgifterna isär.

LOPPSI 2 är den engelska förkortningen av ett lagförslag som mer allmänt syftar till brottsbekämpning via Internet. Det presenterades offentligt i juni 2009 och ska enligt preliminära uppgifter behandlas i parlamentet någon gång under första halvåret 2010. Förslaget har väckt störst uppmärksamhet därför att det möjliggör för polisen att placera spionprogram i misstänkta personers datorer,

52 http://en.wikipedia.org/wiki/LICRA_v._Yahoo!

53 Ström 2009, sid 23

54 Riksdag och Departement 2009-11-25. http://www.rod.se/politikomraden/eu/Tvist-om-tolkning-av-telekompaket/

program som sedan levererar detaljerad information om vad vederbörande gör med datorn. I LOPPSI 2 finns dock också en bestämmelse som kan tvinga Internetoperatörer i Frankrike att omedelbart, på order från Inrikesministeriet, blockera material på Internet. Listan över blockerade adresser ska hållas hemlig.[55]

Enligt en statlig svensk utredning (*En framtida spelreglering* SOU 2008:124) har man också i Frankrike bestämt sig för att blockera utländska webbplatser för spel:

"Frankrike arbetar med en ny spelreglering som bygger på samma grundtankar som den italienska, det vill säga öppna en nationell spelmarknad på Internet för nya aktörer och samtidig införa bl.a. blockeringar för utländska webbsidor."[56]

(Om den italienska modellen, se nästa sida.)

Indien

"Indiens regering anser sig … ha befogenhet att utan närmare förklaring tvinga Internetoperatörer i landet att blockera webbadresser om det framstår som nödvändigt …"

Indiens regering anser sig enligt ett beslut från 2003 ha befogenhet att utan närmare förklaring tvinga Internetoperatörer i landet att blockera webbadresser om det framstår som nödvändigt för att upprätthålla Indiens suveränitet, statens säkerhet, vänskapliga förbindelser med främmande länder, allmän säkerhet eller för att hindra uppvigling till brott. Under 2004 och 2005 utnyttjade regeringen denna möjlighet vid ett fåtal tillfällen, i första hand för att blockera pornografi.

Sommaren 2006, efter ett bombdåd mot ett pendeltåg utanför staden Mumbai, beslöt dock regeringen om blockering av 17 webbadresser med utpräglat politiskt innehåll.[57]

När forskarna inom ONI sedan dess har försökt kartlägga filtrerandet i Indien har resultaten delvis varit svårtolkade. Det är uppenbart att regeringen fortsätter att utnyttja sin möjlighet att beordra blockering, men också att det sker i begränsad utsträckning och att långtifrån alla Internetoperatörer följer instruktionerna. De blocke-

55 http://www.edri.org/edri-gram/number7.11/france-law-on-spying

56 SOU 2008:124, sid 431.

57 http://news.bbc.co.uk/2/hi/south_asia/5194172.stm Se också Ström 2009, sid 24.

rade webbadresser som ONI-forskarna hittade hade ett politiskt innehåll. Pornografi blockerades inte längre.[58]

Italien

Från och med 2007 filtreras, enligt ett regeringsbeslut, barnpornografi även i Italien. En statlig myndighet förser Internetoperatörerna med listor över de webbadresser som ska blockeras.[59]

I Italien blockeras också utländska webbplatser för spel. Systemet beskrivs i en statlig svensk utredning:

”Spelutredningen har vid besök hos den organisation som i Italien ansvarar för bl.a. sådana uppgifter som Lotteriinspektionen utför i Sverige, Amministrazione autonoma dei monopoli di Stato (AAMS), inhämtat uppgifter om det system för blockering av speltjänster som tillämpas i Italien sedan snart två år. Italien har valt att blockera domännamn och IP-nummer, det vill säga ett DNS-filter och IP-filter. De Internet- och telekommunikationsföretag i Italien som tillhandahåller den primära uppkopplingen för italienska användare i Italien får en gång per månad en lista med 1 300 domännamn (september 2008) och tillhörande IP-adresser. Listan görs tillgänglig för Internetleverantörer på AAMS webbsida. Kommunikationsföretagen är skyldiga enligt lag att tillämpa blockeringen och ska då någon söker en blockerad webbplats koppla om användaren till en särskild informationssida på AAMS server.

(…)

Att kommunikationsföretagen i Italien tillämpar aktuell blockeringslista övervakas med hjälp av särskilt av AAMS utvecklad programvara. Övervakningen utförs av Finanspolisen och motsvarigheten till Post- och telestyrelsen.

Varje konstaterat fall då ett kommunikationsföretag har släppt igenom en användare till en webbsida som borde varit blockerad enligt listan, innebär att kommunikationsföretaget måste betala en sanktionsavgift som uppgår till mellan 30 000 och 80 000 €.”[60]

---

58 Deibert/Palfrey/Rohozinski/Zittrain, 2008. Sid 289–290.

59 http://www.edri.org/edrigram/number5.1/italy_blocking Se också Ström 2009, sid 24.

60 SOU 2008:124, sid 425.

Italienska operatörer blockerade också under en kortare period 2008 The Pirate Bay.[61]

Nederländerna

Nederländerna filtrerar sedan 2008 barnpornografi, och har organiserat verksamheten på samma sätt som Sverige. Internetoperatörerna blockerar frivilligt, och får listan över webbadresser från polismyndigheten KLPD (Korps Landelijke Politiediensten).[62]

Norge

Norge filtrerar barnpornografi med samma organisation och samma tekniska lösning som används i Sverige.

Schweiz

En schweizisk domare beordrade 2002 några av landets Internetoperatörer att blockera tre amerikanska webbplatser med stark kritik mot Schweiz rättssystem.[63]

Storbritannien

I Storbritannien filtreras barnpornografi sedan 2004. Internetoperatörerna gör det frivilligt, men den brittiska modellen skiljer sig i vissa avseenden från den svenska, bland annat genom att ingen myndighet är inblandad. Listorna över webbadresser som ska filtreras upprättas av en civil organisation – Internet Watch Foundation, IWF. Även i tekniskt avseende har det brittiska filtret konstruerats annorlunda än det svenska.

---

61 Ström 2009, sid 24.

62 En utvärdering av hur barnporrfiltreringen fungerar i Nederländerna finns på: http://www.wodc.nl/onderzoeksdatabase/internetfilters-tegen-kinderporno.aspx?cp=44&cs=6780. (Språket är holländska, men rapporten rymmer också en sammanfattning på engelska.)
Se också Ström 2009, sid 24.

63 Ström 2009, sid 25.

Sverige

Som redan påpekats filtreras i Sverige barnpornografi sedan 2005. (Hur det organiseras beskrivs mer utförligt under rubriken Filtrering av barnpornografi i Sverige i nästa kapitel.) Verksamheten startades sedan dåvarande justitieministern ställt ultimatum:

"–Om inte branschen tar ansvar för detta tvekar jag inte att ta initiativ till ny lagstiftning, säger justitieminister Thomas Bodström."[64]

Han aviserade några månader senare planer på att gå vidare:

"Nu vill justitieminister Thomas Bodström även ha ett filter för trafficking. Han har uppmanat polisen att tillsammans med internetleverantörer se över hur det här kan genomföras.

–Vi kommer att se till att samarbetet utvecklas på ett sätt att nätleverantörerna får bättre möjlighet att avgöra när det är frågan om koppleri och människohandel, så de kan agera för att få bort de här sidorna så fort som möjligt, säger Thomas Bodström till Ekot."[65]

Hur det skulle ha fungerat i praktiken framgick inte av hans uttalanden. Bodström tog dock inga konkreta politiska initiativ i frågan innan den socialdemokratiska regeringen tvingades avgå efter valet 2006, och den nya borgerliga har inte visat något intresse för saken.

Däremot väckte alliansregeringen 2007 frågan om filtrering i ett annat sammanhang. I en riksdagsskrivelse lanseras tanken att man borde kunna komma åt "terroristvänligt material" genom operatörernas frivilliga agerande:

"Uppmaningar till våld sprids allt oftare via Internet. Någon möjlighet för det allmänna att tvinga operatörer att blockera en webbsida på grund av dess innehåll finns inte och att föreskriva en sådan är svårförenligt med svensk yttrande- och tryckfrihetslagstiftning. Frivilliga åtgärder från operatörernas sida i samarbete med polisen är en möjlig väg, till exempel med förebild i det arbete som skett för att stävja spridning av barnpornografi på Internet. Europol har nyligen startat ett projekt för att samla erfarenheter och lös-

64 Dagens Nyheters nätupplaga 2005-03-11. http://www.dn.se/nyheter/sverige/telia-tvarvander-om-barnporrfilter-1.368333

65 Dagens Nyheters nätupplaga 2005-06-27. http://www.dn.se/nyheter/sverige/trafficking-via-internet-ska-stoppas-1.361624

ningar från olika länder i syfte att utveckla det internationella samarbetet."[66]

Den statliga Spelutredningen föreslog i december 2008 att Internetoperatörerna skulle bli skyldiga att filtrera bort webbplatser med utländska lotterier vilkas verksamhet inte är anpassad efter svensk lag. Förmedling av insatser via sådana webbplatser skulle förbjudas och filtreringen skulle ske genom blockering av både IP-nummer och domännamn.[67] Förslaget mötte åtskillig kritik, och huruvida regeringen ska gå vidare med det är fortfarande, ett år senare, oklart.

Sydkorea

Forskarna inom Open Net initiative, ONI, sammanfattar 2008 sina undersökningar av den Sydkoreanska statens agerande så här (egen översättning):

"Även om Sydkorea är världsledande vad gäller befolkningens Internetanvändning och utbyggnaden av bredband har medborgarna inte tillgång till ett fritt och ofiltrerat Internet. Staten utövar, i ovanligt hög grad för att vara ett fritt och demokratiskt samhälle, filtrering av Internet. Den begär att Internetoperatörer ska blockera webbplatser på en lista upprättad av regeringen och etablerar en kultur präglad av självcensur genom svepande formuleringar i lagen om att enskilda kan straffas för ha lagt ut "statsfientligt" material på nätet. Staten kräver också att koreanska webbsidor ska märka sitt innehåll och att Internetoperatörer och andra nätaktörer, som Internetcaféer och skolor, aktivt ska arbeta på att få bort innehåll som kan anses skadligt för unga. Det har förekommit uppgifter om att den sydkoreanska regeringen ska sluta filtrera webbplatser med material som är positivt till Nordkorea, men ONI:s tester visar att man

66 Regeringens skrivelse 2007/08:64. Nationellt ansvar och internationellt engagemang – En nationell strategi för att möta hotet från terrorism. http://www.sakerhetspolisen.se/download/18.5bf42a901201f330faf80001761/strategihotfranterrorsism.pdf

67 SOU 2008:124. Utredningen kan laddas ned från: http://www.sweden.gov.se/sb/d/10283/a/117594

fortfarande filtrerar stora mängder information som rör Nordkorea, liksom ett antal webbplatser för spel och piratkopierade datorprogram."[68]

Tyskland

"Att förbjuda påståenden om historiska händelser vore otänkbart i USA, även när påståendena är uppenbart felaktiga, men anses nödvändigt i Tyskland."

Även de stater som utan reservationer brukar definieras som demokratier kan, som redan har framgått, i viktiga avseenden skilja sig åt i synen på yttrandefrihet. Om USA är ett land där yttrandefriheten får väga tungt gentemot andra samhälleliga intressen, blir resultatet av motsvarande avvägningar i Tyskland ofta ett annat. Att förbjuda påståenden om historiska händelser vore otänkbart i USA, även när påståendena är uppenbart felaktiga, men anses nödvändigt i Tyskland.

Skillnaden kan också illustreras med en rättstvist som uppstod i Tyskland 2009 när den tyska redaktionen för uppslagsverket Wikipedia tvingades, ställda inför hot om stämning, ta bort namnen på två personer som 1990 dömdes för mordet på den kände skådespelaren Walter Sedlmayer. Mördarna hade då avtjänat ett 15-årigt fängelsestraff, det vill säga sonat sitt brott, och skulle enligt tysk rätt slippa fortsatt publicitet i saken.

Redaktionen för den engelskspråkiga delen av Wikipedia – som naturligtvis också är tillgänglig i Tyskland – såg dock ingen anledning att ta bort några namn. De tyska advokaterna har stämt Wikipedia inför tysk domstol och i skrivande stund (december 2009) är målet inte avgjort.[69]

Tidigare (2000 och 2002) har tyska domstolar på delstatsnivå beordrat Internetoperatörer att blockera utländska webbplatser med nazistiskt innehåll.

Från den 1 januari 2008 gäller i Tyskland ny spellagstiftning som generellt förbjuder spel via Internet. Som motiv anges risken för

68 Deibert/Palfrey/Rohozinski/Zittrain. *Access Denied. The Practice and Policy of Global Internet Filtering*. (Tillträde förbjudet. Praktik och politik för världsomspännande Internetfiltrering.) The MIT Press 2008. Sid 372–373.
Även på: http://opennet.net/research/profiles/south-korea

69 http://www.nytimes.com/2009/11/13/us/13wiki.html?_r=1

spelberoende.[70] Ännu i december 2009 tycks dock oklarhet råda hur man ska försäkra sig om att förbudet efterlevs – till exempel om filtrering ska användas.

Turkiet

En åklagare gav 2007 order om att internetsajten Youtube skulle blockeras för nätsurfare i Turkiet. Åklagarmyndigheten hävdade att landsfadern Mustafa Kemal Atatürk förolämpades i videofilmer som publiceras på Youtube.[71]

USA

USA var först med upprörda debatter, politiska strider och domstolsbeslut om filtrering av Internet – men då gällde det inte filtrering på operatörsnivå. Den ordning som nu har utmejslats återspeglar landets politiska kultur. Å ena sidan anses det självklart att barn och ungdom måste skyddas från sex och nakenhet, å andra sidan är det svårt att på federal nivå (det vill säga presidenten, regeringen och parlamentet) fatta beslut som innebär inskränkningar i yttrandefriheten.

Huvudansvaret för att skydda barn läggs därmed dels på föräldrar och andra vuxna som förväntas sköta eventuell filtrering via den egna datorn, dels på offentliga inrättningar som skolor och bibliotek. En stor marknad för PC-baserade filtreringsprogram har uppstått, men användare kan också nöja sig med *”SafeSearch”*-lösningar som sökmotorn erbjuder. Google har en sådan. En ”porrsäker” version av till exempel Google innebär alltså att den användare som redan känner till en porrsidas webbadress kan skriva in den i adressfältet och därmed enkelt nå den, men att han/hon inte kan hitta den med sökmotorns hjälp.

24 av USA:s 50 delstater har lagregler med relevans för filtrering i offentligt finansierade skolor eller bibliotek. I flertalet av dessa stater krävs helt enkelt att skolor respektive bibliotek beslutar om en policy som syftar till att hindra barn från att komma åt utpräglat

70 SOU 2008:124, sid 242.

71 TT-AP-telegram publicerat i Dagens Nyheter 2007-03-07.

sexuellt, obscent eller annat skadligt material. Några stater har dock mer detaljerade krav på filtrering.[72]

På federal nivå har länge pågått en kraftmätning mellan kongressen, som med konservativa politiker i spetsen drivit fram lagstiftning för att på olika sätt avskärma det amerikanska samhället men framför allt barn och ungdom från nakenhet, och medborgarrättsorganisationer som American Civil Liberties Union, ACLU, och Electronic Frontier Foundation, EFF. De senare har, ofta tillsammans med bibliotekariernas organisation American Library Association, ALA, drivit mål i domstolarna i syfte att få ny, censurerande lagstiftning underkänd såsom stridande mot det första tillägget i konstitutionen – det som ska garantera yttrandefriheten. Huvudargumentet mot sådan lagstiftning är att den oundvikligen leder till överblockering, det vill säga att även material som inte är pornografiskt stoppas. Filtren tycks alltid blockera också mycken debatt i moralfrågor och saklig information om sådant som sexualitet och könssjukdomar.

På 1990-talet vann medborgarrättsorganisationerna en uppmärksammad strid i domstolarna om The Communications Decency Act, CDA, som i högsta instans (Högsta Domstolen) ansågs oförenlig med konstitutionen. De konservativa krafterna i kongressen återkom dock med en modifierad version – The Childrens Internet Protection Act, CIPA. Den lagen antogs 2000 och har sedan dess stått emot attackerna. Där stadgas bland annat att bibliotek bara kan få offentliga bidrag om de kan visa att de använder filterprogram som förhindrar att unga konfronteras med obsceniteter, barnpornografi eller annat material som är skadligt. I ett uppmärksammat CIPA-mål (United States v. American Library Association) bedömde Högsta Domstolen 2003 att lagen inte stred mot konstitutionen eftersom biblioteken var tillåtna att, på vuxna Internetanvändares begäran, stänga av filtret. Därför spelade det enligt domstolen mindre roll att filtren i betydande utsträckning överblockerade, det vill säga stoppade mer än man egentligen önskade.[73]

72 För en översikt över delstatlig reglering i USA, se: http://www.ncsl.org/programs/lis/CIP/filterlaws.htm

73 Se: http://www.ncsl.org/programs/lis/CIP/filterlaws.htm

Illustration: © Camilla Laghammar

Filter och lagar

Det här kapitlet fokuserar på juridiken. I vilken utsträckning kan operatörerna, den svenska riksdagen, EU eller Europadomstolen besluta om den typ av censur som filtrering innebär?

Möjligheterna att utnyttja Internet förändras hela tiden. Det gör också den tekniska plattformen som sådan. Internet är ju på sätt och vis ”bara” programvara, och hur systemet kan användas beror på dess bärande element i form av protokoll och standarder. Vad denna tekniska plattform möjliggör, försvårar eller omöjliggör bestämmer människor som underhåller, renoverar och moderniserar den. Om och när Internetanvändares identitet eller geografiska position ska kunna fastställas av andra aktörer till exempel, är avhängigt tekniska val.

I samhällen som blivit höggradigt beroende av tekniska kommunikationssystem kan därmed programmering vara ett lika effektivt styrmedel som lagstiftning – eller ännu effektivare. En ofta använd liknelse handlar om hur man ska få bilförare att sänka farten på ett visst vägavsnitt. Man kan placera ut 30-skyltar, det vill säga med lag förbjuda höga hastigheter, eller bygga asfalttrösklar, det vill säga med tekniska medel tvinga förarna att sakta ned. Tvång med teknik blir här avsevärt effektivare än tvång med lag. Så är det i många sammanhang. De som kan påverka våra kommunikationssystems tekniska utformning kan, åtminstone i vissa avseenden, påverka medborgarnas möjligheter att utnyttja yttrande- och informationsfriheterna.[74]

74 Den som vill fördjupa sig i sådana frågor rekommenderas bland annat: Kesan, Jay P/Shah, Rajiv C. *Deconstructing Code*. Yale Journal of Law & Technology, Vol. 6, 2003–2004, s. 277 ff,. (Kan nedladdas från: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=597543)
Se också: Lessig, Lawrence. *Code and other Laws of Cyberspace*. New York 1999.

Drömmen om Vilda Västern

Kring alla former av maktutövning – såväl teknisk som ekonomisk som juridisk – tycks missuppfattningar och mytbildning uppstå. En föreställning som ofta skymtat i de senaste 15 årens diskussioner om Internet är att lagar med nödvändighet utgör inskränkningar i medborgarnas frihet. Själva laglösheten, som den i Vilda västern, framställs som ett ideal, ibland till och med som liktydigt med frihet. I Vilda västern var medborgaren fri på riktigt, är tanken – fullständigt oberoende och litande endast till sig själv.

Parallellen mellan Vilda Västern och ”cyberspace” användes särskilt flitigt på 1990-talet, när rockmusikern John Perry Barlow och IT-miljardären Mitch Kapor startade medborgarrättsorganisationen The Electronic Frontier Foundation, EFF. Namnet The Frontier syftade på de områden som nybyggare ännu inte hade koloniserat – där marken var gratis och man kunde leva fri. (Indianerna brukar som bekant vara frånvarande i den politiskt kraftfulla amerikanska Vilda Västern-myten.) Där fanns inga lagar, inga poliser, ingen beskattning, inga påbud från överheten. Barlow och Kapor utgick från Internet som en ny gränslös livssfär, fri att kolonisera och omöjlig för den fysiska världens makthavare att kontrollera. Varje försök till lagreglering av cyberspace skulle misslyckas och bara ställa till skada, hävdade de. På det ideologiska planet kan detta förhållningssätt, som man ofta möter i USA men tidvis också i Sverige, bäst beskrivas som högeranarkism. Lagar stiftas, i denna föreställningsvärld, av en överhet som per definition är inkompetent, dominerad av särintressen, korrupt och mer eller mindre förtryckande.

”Barlow och Kapor utgick från Internet som en ny gränslös livssfär, fri att kolonisera och omöjlig för den fysiska världens makthavare att kontrollera.”

Allt eftersom åren har gått och Internet utvecklats har radikaler av Barlows och Kapors typ dock tvingats tala med allt mindre bokstäver. För den som bortser från utopierna och fokuserar på den verkliga världen blir det uppenbart att en lag lika gärna kan fungera befriande som förtryckande. En värld fri från lagar ger i praktiken – de historiska erfarenheterna är alldeles entydiga – frihet bara åt de starkaste. Våra grundlagar om yttrandefrihet till exempel – tryckfrihetsförordningen och yttrandefrihetsgrundlagen – är till stora delar riktade *mot* staten, det vill säga lagreglerna begränsar statens

möjligheter att ingripa mot medborgarna och säkrar därmed enskildas frihet att uttala sig kritiskt och utmanande. Utan lagens stöd är den enskilde i många sammanhang hjälp- och rättslös.

Ett mediums ”gränslöshet” är heller inget som talar mot att det skulle lagregleras. Vi har haft gränsöverskridande etermedier i ett halvt sekel utan att någon har ifrågasatt riksdagens rätt att stifta lagar om radio- och tevesändningar i Sverige.

För den som vill värna demokratiska fri- och rättigheter blir frågan därmed inte om staten – hittills nationalstaten, i framtiden kanske EU-staten – ska ingripa mot misstänkt brottslighet som pågår med hjälp av Internet. Frågan är *hur* sådan brottsbekämpning ska gå till.

Alla svenska samhällsdebattörer av betydelse tycks idag vara inne på den linjen, även om de är oense om vad som faktiskt bör göras. Pendeln har svängt, kanske har den till och med svängt för långt. Om högeranarkismen på 1990-talet försvårade en förnuftig diskussion om lagregler och Internet, tycks risken 2010 snarast vara att kontrollambitionerna får alltför stort spelrum. På 1990-talet beskrevs Internet vanligen som fritt, modernt och grunden för en ny samhällsekonomi. På senare år är tendensen snarare att betona nätets farlighet – som en arena för pedofiler och grov organiserad brottslighet, för prostitution, våld, piratkopiering och illvilliga människor som gräver i varandras privatliv. Istället för frihet från lagar riskerar vi därmed att lägga grunden till alltför många och frihetsinskränkande lagar. Vågen av nya och förstärkta statliga – särskilt polisiära – tvångsmedel är hårt kritiserad men har inte i någon större utsträckning kunnat hejdas.

Nu går det naturligtvis inte att reducera frågan om framtida brottsbekämpning till att handla endast om antalet lagar, eller ens antalet integritetskränkande lagar. De viktiga variablerna är fler än så.

Vem äger? Vem bestämmer?

En central fråga är vem som faktiskt har kontroll över Internet.

”Ingen” var länge, i Barlows och Kapors anda, standardsvaret på frågan. Nätet sträcker sig över alla gränser. Ingen regering, inget

internationellt organ kan kontrollera det. Internet är både globalt i utsträckning och maximalt decentraliserat. Användarna, ingen central instans, bestämmer tillsammans innehållet.

Det är naturligtvis sant, men långtifrån hela sanningen. Två amerikanska juridikprofessorer, Jack Goldsmith och Tim Wu, skrev 2006 en bok där de målade upp hela (eller nästan hela) bilden.[75] Som påpekades i inledningen till denna guide kan nationalstaten, men också andra maktcentra, påverka och prägla verksamheten på Internet på många sätt.

Gränsöverskridande regler för gränsöverskridande nät?

När nu Internets oberoende av nationsgränser skapar så stora problem, även djup oenighet mellan parlamentariska demokratier som USA å ena sidan och Frankrike och Tyskland å den andra, borde inte frågan om tillåtet respektive otillåtet på nätet besvaras genom internationella överenskommelser? Sådana har förhandlats fram i andra sammanhang. Genom konventioner bestäms nu vad som gäller i rymden, inom luft- och sjöfart, på havsbottnarna, för teletrafik, patent, handel och till och med vad krigförande länder får och inte får göra. Varför inte söka en lösning av samma slag om tillåtet och otillåtet på Internet?

Förslaget om en internationell överenskommelse har aldrig lanserats på allvar av någon nation eller internationell organisation. Ett skäl är naturligtvis att demokratier skulle få svårt att enas med diktaturer, men sannolikt skulle även demokratierna inbördes få svårt att komma överens. Lagregler på detta område är djupt förankrade i en nationell eller regional kultur som i sin tur präglas av sådant som religiösa övertygelser, traditioner och historiska erfarenheter. De sociala normerna om anständigt och oanständigt, acceptabelt och oacceptabelt, om vad staten ska göra och vad staten måste

”… demokratier skulle få svårt att enas med diktaturer, men sannolikt skulle även demokratierna inbördes få svårt att komma överens.”

75 Goldsmith, Jack/Wu, Tim. *Who Controls the Internet? Illusions of a Borderless World.* Oxford University Press, 2006.

hålla sig borta från skiljer sig påtagligt även mellan de länder som definieras som demokratier.

Man kan hypotetiskt föreställa sig en internationell konferens, kanske i FN:s regi, med målet att enas om yttrandefrihetens gränser på Internet. Varje delegat på en sådan konferens skulle av den egna regeringen förses med ett begränsat mandat att förhandla. Alla skulle komma till konferensen med instruktioner om det icke förhandlingsbara. Flertalet diktaturer skulle vägra acceptera en överenskommelse som garanterade oppositionella fritt spelrum. Många muslimskt dominerade länder, men också åtskilliga kristna, skulle kräva möjligheter att ingripa mot hädelse. En del katolska länder skulle motsätta sig information om/tjänster för kvinnor som vill göra abort. Vissa stater skulle hävda att uttryck för rasism eller information som kan underlätta för terrorister måste bannlysas. Åtskilliga länder skulle fordra förbud mot pornografi, andra skulle nöja sig med att kunna ingripa mot vissa särskilt anstötliga former av den – och hur det anstötliga definierades skulle variera. Det enda man idag möjligen kunde enas om vore ett förbud mot barnpornografi, låt vara att åsikterna skulle gå isär om vad som är ”pornografiskt” och var åldersgränsen för ”barn” går.

Uppräkningen av de företeelser som framstår som oacceptabla för åtminstone någon stat skulle bli lång. Om alla delegater vid förhandlingarna finge gehör för sina krav på undantag för det oacceptabla skulle konventionen alltså bara garantera yttrandefrihet för det mest harmlösa Internetinnehållet, det vill säga den skulle inte garantera någon yttrandefrihet värd namnet. Funktionen skulle snarast bli den omvända. Konventionen skulle legitimera omfattande inskränkningar i yttrandefriheten. Med alla sina undantag utgjorde den ju ett veritabelt smörgåsbord av censureringsmotiv.

Totalitärt styrda stater har ingen anledning att ge sig in i förhandlingar om en internationell yttrandefrihetskonvention. Stater som tar medborgerliga rättigheter på större allvar inser att konventionen, om en sådan överhuvudtaget kunde utarbetas, snarast skulle riskera att motverka syftet. Följaktligen har världens länder, 15 år efter att Internet blivit tillgängligt för vanliga användare, inte ens

diskuterat någon form av internationella överenskommelser på yttrande- och informationsfrihetens område.

Vad hindrar då att de äldre deklarationerna om fri- och rättigheter som formulerats inom FN och genom Europarådet – där yttrandefriheten framställs som central – tillämpas på Internet? I princip ingenting, men i praktiken är det svårt. Deklarationerna talar visserligen om allas rätt till yttrandefrihet och informationsfrihet, men säger också att friheterna får inskränkas med hänvisning till en rad övergripande intressen som till exempel statens säkerhet, behovet att förebygga brott eller samhällelig oordning, att skydda hälsa och moral, att skydda enskildas goda namn och rykte med mera. Dessa undantagsmöjligheter åberopas och utnyttjas nu med stor uppfinnings- och variationsrikedom världen över. Det är nog orättvist att kalla FN-deklarationens och Europadeklarationens avsnitt om yttrandefrihet för ”smörgåsbord av censureringsmotiv”, men man kan heller inte beskriva dem som särskilt effektiva vapen i försvaret av yttrandefriheten på de platser där den är hotad eller helt avskaffad.

För Sveriges och Europas del kan dock med tiden – även om det inte går att säga med säkerhet – Europakonventionen om mänskliga rättigheter med tiden få ett genomslag på Internet. Mer om detta längre fram.

Internetkontroll i auktoritära stater

Internet har ända sedan födseln beskrivits som ett hot mot totalitära regimer. Med webben och e-post förlorar de möjligheterna att styra och kontrollera informationsflöden. Censur och statlig propaganda upphör att fungera och därmed, förr eller senare, diktaturerna själva. Sådan argumentering saknar naturligtvis inte helt grund, men tenderar hos många debattörer att övergå i önsketänkande. USA:s förre president Ronald Reagan hävdade i ett tal i London 1989:

”Tekniken kommer att göra det allt svårare för stater att kontrollera vilken

information folket kan ta emot. (…) Totalitarismens Goliat kommer att besegras av mikrochipets David."[76]

Två amerikanska forskare, Shanti Kalathil och Taylor C. Boas visade i studie publicerad 2003 att dessa förväntningar (dittills) inte hade infriats. Visst finns det exempel på att filmbilder och annan information om totalitära regimers brutala behandling av oppositionella har kunnat spridas snabbt via Internet, vilket bidragit till ökat internationellt tryck på de ansvariga, men det finns knappast något fall där "mikrochipets David" därmed har vunnit striden. I boken Open Networks, Closed Regimes (Öppna nätverk, stängda regimer) visade Kalathil/Boas att Internet, som all annan teknologi, kan nyttjas för vitt skilda syften. Demokrati uppstår genom människors organisering och målmedvetna kamp, inte med någon automatik ur ett tekniskt system.[77]

"Demokrati uppstår genom människors organisering och målmedvetna kamp, inte med någon automatik ur ett tekniskt system."

Nyhetsmedier förmedlar ofta en grovt förenklad bild av totalitära regimer. Att det statliga styret är totalitärt betyder inte att det är okomplicerat. Inte ens de mest demoniserade av diktatorer – en Pol Pot eller en Saddam Hussein – har haft makt över allt och alla. Diktatorn är alltid en central aktör, men han är aldrig ensam på den nationella scenen. Han måste fortlöpande försäkra sig – minst lika ofta med morot som med piska – om stöd och lojalitet från sitt samhälles olika institutioner och sociala skikt. För regimens överlevnad på längre sikt måste ekonomin fungera åtminstone hyggligt. Globala och regionala stormakter driver hela tiden ett maktspel som för de styrande i mindre länder fortlöpande skapar nya risker och nya möjligheter. När en ny kommunikationsteknologi som Internet börjar genomtränga samhällen och nationer öppnar sig för dess makthavare handlingsalternativ som är lika svåra att utvärdera för diktatorn som för den demokratiskt valde ledaren. Det finns knappast några självklara "effekter" av Internet – på ekonomisk utveckling, på demokratiska processer, på utbildning, på sociala motsättningar.

76 Kalathil, Shanti/Boas, Taylor C. *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule.* Carnegie Endowment for International Peace, 2003. Sid 1.

77 Kalathil, Shanti/Boas, Taylor C. A a.

Kina har idag fler Internetanvändare än något annat land. Ledningen för det styrande kommunistpartiet definierade redan i slutet av 1980-talet telekommunikation som ett strategiskt – i ekonomiskt avseende – viktigt område. Stora pengar satsas sedan dess på system- och kompetensuppbyggnad, men också på att organisera stark statlig styrning. Sedan 1996 försöker man att både stimulera och kontrollera medborgarnas Internetanvändning. Det tycks än så länge vara en relativt framgångsrik strategi.

”Vidare genomförs med ojämna mellanrum kraftfulla polisiära tillslag mot ”missbruk” av Internet som resulterar i hårda domar. ”… Avsikten är att skrämma människor till självcensur.”

Kontrollen utövas på flera plan och på flera sätt, där filtrering bara är ett inslag av många, låt vara ett av de viktigaste. Företag som erbjuder Internetuppkopplingar måste ha aktiva censorer och de många Internetcaféerna måste vaka över sina kunders surfande, chattande etcetera. Vidare genomförs med ojämna mellanrum kraftfulla polisiära tillslag mot ”missbruk” av Internet som resulterar i hårda domar. Detta rapporteras också i de statskontrollerade nyhetsmedierna. Avsikten är att skrämma människor till självcensur.

I länder med andra förutsättningar väljs andra strategier. Kuba till exempel, har inte som Kina en hyggligt välbeställd medelklass som kan bära upp större kommersiella företag inom Internetsektorn. Även Kuba formulerade, skriver Kalathil/Boas, relativt tidigt (med Internetmått mätt) statliga mål för ”informatisering” av landet. Att såväl IT i allmänhet som Internet i synnerhet öppnade stora möjligheter för samhällelig utveckling konstaterade regeringen 1997. Till skillnad från Kina har man i Kuba inte valt att stimulera enskilda medborgares Internetanvändning utan ger Internettillstånd till pålitliga företag, institutioner och organisationer vars ledare sedan har kontrollansvaret. Några storskaliga försök att inom landet blockera/filtrera bort olämpliga webbplatser har inte gjorts.

Den kubanska ledningens strategi har hittills varit framgångsrik. Det är fullt möjligt att Kubas regim småningom faller, skriver Kalathil/Boas, men inget tydde 2003, då boken skrevs, på att Internet skulle få någon större betydelse i en sådan utveckling.

Slutsatserna blir i stort sett desamma för övriga granskade länder, trots deras stora inbördes olikheter: Burma, Vietnam, Singapore, Arabemiraten, Saudiarabien och Egypten. Såväl i det rika och välutbildade Singapore som det fattiga Vietnam har, enligt Kalathil/

Boas, människor tillåtits utnyttja Internets möjligheter – tekniskt och ekonomiskt – samtidigt som regimerna har kunnat undvika de politiskt befriande effekter som Reagan med flera talade om.

Olikheter mellan länderna kan inte bara förklaras med skillnader i ekonomiska resurser. Varje hierarkisk maktstruktur vilar på sin egen historiska och kulturella grund. En auktoritär regim kan av olika skäl tolereras eller till och med vara populär i breda folklager. Ett skäl kan helt enkelt vara att de realistiska alternativen till den uppfattas som värre. Kalathil/Boas studie av arabvärlden visar att Förenade Arabemiraten och Saudiarabien satsat stora resurser på att censurera Internet, medan Egypten varken censurerar eller försöker begränsa invånarnas möjligheter att koppla upp sig. Likväl tycks Internet lika litet ”underminera” Mubarak-regimen i Egypten som någon av de andra.

Internetkontroll i parlamentariska demokratier

Sätten att besluta om och organisera filtrering varierar i alla stater. Rollfördelningen mellan lagstiftare och privata aktörer är aldrig given. Internet- och telekomföretagen har dock en nyckelroll eftersom de i praktiken kontrollerar så stora delar av nätets hård- och mjukvara. Nästan alla ledande politiker i de parlamentariska demokratierna ser helst, som Thomas Bodström i Sverige 2005, att Internetoperatörer ”tar sitt ansvar” och filtrerar bort OM så att politiska beslut om censur kan undvikas.

När Internetburen information av något skäl ska stoppas finns det ju också andra metoder än filtrering att ta till. I flera europeiska länder är känsligheten särskilt stor för nazisters yttranden, till exempel sådana som förnekar eller bagatelliserar nazi-Tysklands folkmord på judar, romer och andra grupper som ansågs mindervärdiga. Både tyska och franska domstolar har krävt att de ansvariga för portaler eller webbplatser med ett innehåll som är olagligt i respektive land ska blockera personer som från Tyskland respektive Frankrike försöker komma åt innehållet.

Här utkräver domstolarna alltså ansvar av personer/företag bakom

enskilda webbplatser i stället för att begära filtrering på högre nivå i nätet. Det kan också gälla webbplatser som erbjuder program med vars hjälp kopieringsskydd kan genombrytas. En tysk webbplats för IT-nyheter – Heise Online – förbjöds hösten 2005 att länka till Slysoft.com, ett Antigua-baserat företag som sålde bland annat datorprogram med vars hjälp man kunde knäcka kopieringsskydd för CD- och DVD-skivor.[78]

Under förutsättning att den innehållsansvarige finns i landet eller har materiella tillgångar där – och följaktligen kan nås med straffrättsliga åtgärder – kan lagstiftaren nå ganska långt genom att rikta krav mot den ansvarige för webbplatsen. När personen/företaget/organisationen finns utomlands är den nationella domstolens möjligheter att påverka betydligt mindre. Filtrering på operatörsnivå framstår då som ett effektivare medel.

Ett exempel på filtrering i den privata sektorn är också värt att uppmärksamma. I juli 2005 blockerade den kanadensiska Internetleverantören Telus en webbplats tillhörande en fackförening som organiserade vissa av Telus egna anställda. En dispyt mellan företaget och fackföreningen hade uppstått, och när Telus blockerade det IP-nummer som fackföreningen använde blockerades samtidigt 766 webbsidor med innehåll som inte på något sätt hade med tvisten att göra. Företagets åtgärd vållade en del uppmärksamhet, och efter tre dagar hävdes blockeringen av IP-numret. Telus deklarerade dock att man ansåg sig ha en principiell rätt att blockera.[79]

Vad säger internationell rätt?

Rättsliga analyser som tar sikte på Internetbaserad verksamhet handlar ofta om jurisdiktionsfrågor, det vill säga om vilket lands lag som ska tillämpas. Sådana har viss relevans även för filtrering, men är för närvarande inte huvudsaken. Filtrering sker idag nästan alltid för lokala eller nationella syften. Att nationella domstolar har juris-

78 http://www.immateriblog.de/archives/000254.html

79 http://opennet.net/bulletins/010/

diktion över de fysiska tele- och datanät som finns i landet – och i vilka information blockeras – kan knappast ifrågasättas. När information som förklarats illegal i land A har sitt ursprung i land B kan filtrering i land A snarast bli den metod för ingripande som förefaller attraktivast just därför att den inte medför jurisdiktionsproblem.

"Man kan naturligtvis tänka sig att information som kommuniceras mellan land A och land B, där den i båda fallen är laglig, blockeras i mellanliggande länder genom vilka dataströmmarna vidarebefordras."

Att den internationella tele- och datatrafiken i hög grad bygger på samarbete och internationella överenskommelser är självklart, men sannolikheten för att filtrering ska försvåra sådant samarbete förefaller inte stor. Man kan naturligtvis tänka sig att information som kommuniceras mellan land A och land B, där den i båda fallen är laglig, blockeras i mellanliggande länder genom vilka dataströmmarna vidarebefordras. Konflikter av det slaget tycks ännu inte ha uppkommit, och med tanke på att Internets själva grundkonstruktion syftar till att bevara funktionaliteten i systemet även när enskilda noder har slagits ut förefaller risken för sådana incidenter liten. Om datatrafiken mellan land A och land B stoppas i land C kommer Internet alltså normalt att förmedla den längs andra vägar.

Filtrering aktualiserar däremot en rad yttrande- och informationsfrihetsfrågor. De internationella regelverk som har störst relevans i sammanhanget torde vara *FN:s allmänna förklaring om de mänskliga rättigheterna* och *Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna*.

FN-deklarationens artikel 19 talar om envars rätt till åsiktsfrihet och yttrandefrihet. *"Denna rätt innefattar frihet för envar att utan ingripanden hysa åsikter och frihet att söka, mottaga och sprida upplysningar och tankar genom varje slags uttrycksmedel och utan hänsyn till gränser."* I praktiken är dock FN-deklarationens garanti mer moraliskt än juridiskt förpliktande. Svenska domstolar kan inte döma med stöd av den, och någon mekanism för att tvinga de länder som ratificerat konventionen att också i praktiken följa den finns inte.

Europakonventionen väger då tyngre. Den slår i artikel 10 fast att allas rätt till yttrandefrihet: *"...innefattar åsiktsfrihet samt frihet att mottaga och sprida uppgifter och tankar utan inblandning av offentlig myndighet och oberoende av territoriella gränser."* Eftersom filtrering inte syftar till att hindra någon från att yttra sig utan tar sikte på att hindra vissa gruppers mottagande av yttranden, är det begreppen

”frihet att … mottaga … upplysningar och tankar” som här står i centrum. Hur ska denna ”frihet” förstås? Med tanke på att Europa-konventionen sedan 1995 också gäller direkt som svensk lag framstår det som en viktig fråga. Här är bristen på rättsliga analyser och rättsfall uppenbar.

Hans Danelius, justitieråd och expert på Europadomstolens praxis, skriver:

”Yttrandefriheten, så som den skyddas i artikel 10, innebär främst att staten skall avhålla sig från att hindra eller bestraffa fri spridning av tankar och idéer. Det är alltså en negativ förpliktelse – en förpliktelse att inte handla – som åläggs staten.”[80]

Konventionen säger, enligt Danelius, att en stat får besluta om begränsningar i informationsfriheten om

1. det sker med lagstöd,
2. det tillgodoser något av följande ändamål – *”statens säkerhet, den territoriella integriteten, den allmänna säkerheten, förebyggande av oordning eller brott, skyddande av hälsa och moral eller av annans goda namn och rykte eller rättigheter, förhindrande av att förtroliga underrättelser sprids eller upprätthållande av domstolarnas auktoritet och opartiskhet”*,
3. det är nödvändigt i ett demokratiskt samhälle för att tillgodose något av dessa ändamål.[81]

Det låter inte som någon särskilt tydlig inskränkning i staternas rätt att filtrera. Går det att vara mer precis? I den rapport finansierad av The Open Society Institute som nämndes i förra kapitlet argumenterar de fyra forskarna för att (egen översättning):

”Frågan om att balansera grundläggande fri- och rättigheter när de står i konflikt med varandra kräver en detaljerad analys av precis det slag som Europadomstolen för mänskliga rättigheter har utvecklat och som indirekt skapat riktlinjer för hur blockeringsinsatser på Internet kan genomföras om de bedöms vara lämpliga, proportionella och tekniskt genomförbara. I analysen måste man beakta de principer som har sin grund i behovet av allmän ordning

80 Danelius, Hans. *Mänskliga rättigheter i europeisk praxis*. Norstedts Juridik 2007, sid 367.

81 Danelius, Hans. A a sid 368.

och säkerhet och de som innebär att rättighetsinskränkningar bara är godtagbara om de framstår som nödvändiga i ett demokratiskt samhälle. Principerna får ligga till grund för en granskning av målen med olika initiativ till blockering, och en bedömning av hur dessa mål överensstämmer med de riktlinjer Europadomstolen dragit upp."[82]

En slutsats framstår enligt OSI-rapporten som helt klar:

"System för blockering ska antingen inrättas med stöd i nationell lag eller inte inrättas alls. System som utgör branschens självreglering präglas inte av tillräcklig öppenhet och skapar inte möjlighet att utkräva ansvar."[83]

I rapporten utarbetas en slags checklista i tio punkter (delvis överlappande) för kontroll av om blockering av Internetinnehåll kan anses acceptabelt:

1. Kontrollera att Internetblockering, om sådan ska implementeras, inte onödigtvis kränker fri- och rättigheter.
2. Klargör vilka fri- och rättigheter som inskränks genom blockerandet.
3. Klargör hur mycket de inskränks.
4. Klargör tydligt det/de mål som ska uppnås.
5. Visa att målet med blockerandet är realistiskt.
6. Klargör om det finns ett starkt samhälleligt behov av att målet uppnås.
7. Gör en analys av om det statliga ingreppet står i rimlig proportion till målet.
8. Beakta de principer som enligt Europadomstolen måste tillämpas vid blockering ("nödvändigt i ett demokratiskt samhälle" och "starkt samhälleligt behov").

82 Callanan/Gercke/De Marco/Dries-Ziekenheiner: *Internet blocking – balancing cybercrime responses in democratic societies.* Aconite Internet Solutions 2009, sid 35. http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf

83 Callanan med flera, a a sid 36.

9. Fastställ om det är nödvändigt att i lag begränsa hur systemet för blockering får utnyttjas.

10. Stifta lag om det tillåtna blockerandet.[84]

OSI-rapporten är författad av personer med stor teknisk och juridisk sakkunskap. Samtidigt måste sägas att dessa forskare skriver med finansiering från en filtreringsskeptisk organisation och att de i juridisk mening här bryter ny mark. De uttalar sig om hur Europakonventionen ska tillämpas inom ett område där den aldrig tidigare har aktualiserats. Deras tolkning framstår som sympatisk ur yttrandefrihetssynpunkt men att Europadomstolen kommer att nå samma slutsatser är inte självklart. Uppfattningen att blockering av innehåll på Internet behöver ha stöd i nationell lag – att Internetoperatörernas självsanering är oförenlig med Europakonventionen – delas uppenbarligen inte av politiska ledare i länder som Sverige, Danmark, Norge och Storbritannien. De anser tvärtom att självsanering är en utmärkt idé.

Att förutspå hur Europadomstolen kommer att ställa sig till självsaneringen är inte lätt. Danelius konstaterar visserligen i citatet ovan att artikel 10 hittills främst har tolkats som en negativ förpliktelse – som ett krav på att staten ska avstå från att ingripa. Men det finns också exempel på att artikeln har tolkats positivt, det vill säga som ett krav på att enskildas yttrandefrihet ska skyddas mot andra enskilda.

”Fastän artikel 10 primärt ålägger staten att avhålla sig från vissa handlingar, kräver artikeln också att staten genom positiva åtgärder, till exempel genom ändamålsenlig lagstiftning, sörjer för att rätten att sprida tankar och idéer skyddas mot ingrepp från enskilda personer eller institutioner för vilka staten inte bär ett direkt ansvar. Staten bör exempelvis vara skyldig att tillse att spridning av åsikter i samhällsfrågor inte hindras av politiska motståndare och att tidningar kan distribueras utan ingrepp av odemokratiska grupper. I ’Özgür Gündem mot Turkiet’ fann Europadomstolen att de turkiska myndigheterna hade brustit i sin skyldighet enligt artikel 10 att ge

84 Callanan med flera, a a sid 214–218.

en tidning och dess journalister och övriga medarbetare erforderligt skydd mot våldshandlingar och trakasserier."[85]

OSI-rapportens författare har säkert rätt i att Europadomstolen, när den får en tvist om filtrering på sitt bord, behöver göra den typ av avvägningar som framgår av 10-punktslistan tidigare i kapitlet och som påminner mycket om de analyser som Högsta Domstolen i USA tvingades till när The Communications Decency Act och senare The Childrens Internet Protection Act prövades mot konstitutionen. Utgången, när olika mänskliga och samhälleliga värden vägs mot varandra i Europadomstolen, är dock inte given.

Svensk lag och filtrering i Sverige

Sveriges sedan länge etablerade metod för att skydda yttrandefriheten har fungerat väl, anser de allra flesta, men den är också unik. Inget annat land i världen har en juridisk konstruktion för skyddet som liknar vår, och inget har heller så utförliga regler om yttrandefrihet inskrivna i själva grundlagen.

"Inget annat land i världen har en juridisk konstruktion för skyddet som liknar vår, och inget har heller så utförliga regler om yttrandefrihet inskrivna i själva grundlagen."

Sverige blev för nästan 250 år sedan först i världen – vilket var märkligt eftersom landet i övrigt inte var känt som någon hemvist för radikala idéer – med att garantera medborgarna yttrandefrihet i grundlag. Det skedde med Tryckfrihetsförordningen (TF) som trädde i kraft 1766. (Gustaf III avskaffade i praktiken den förordningen några år senare, men sedan 1809 har vi en obruten tradition av grundlagsskydd för yttrandefriheten.) På den traditionen har Sverige sedan byggt vidare. TF har moderniserats i flera omgångar, senast 1949, men de grundläggande principerna har behållits.

TF:s skydd täckte från början bara yttranden som spreds via tryckt skrift – tidningar, pamfletter, böcker – men har sedan utvidgats till att omfatta åtskilligt i form av text och bild som är framställt med annan teknik än tryckpress. Den som gör fler exemplar av en skrift – mångfaldigar den – med hjälp av stencilapparat, kopieringsapparat, datorskrivare eller liknande kan också få grundlagsskydd.

85 Danelius, Hans. *Mänskliga rättigheter i europeisk praxis*. Norstedts Juridik 2007, sid 367.

Det räcker att i skriften tala om att den är framställd i flera exemplar, vem som gjort det och ort/datum för mångfaldigandet.

Sedan 1992 gäller också yttrandefrihetsgrundlagen, YGL, för att ge radio- och teveprogram, videoband, DVD-skivor och liknande ”tekniska upptagningar” samma sorts skydd som TF ger tryckta skrifter. Yttranden som sprids i form av ljud- eller bildupptagningar – det vill säga yttranden som bara kan uppfattas med något tekniskt hjälpmedel – kan därmed också få grundlagsskydd.

Begrepp som *filtrering av information* eller *blockering av information* förekommer nu ingenstans i svensk lag och diskuteras inte i några av lagarnas förarbeten. Det finns av allt att döma, på grund av grundlagsreglerna om yttrande- och informationsfrihet, vissa juridiska hinder för staten att blockera information på Internet. De hindren är dock inte, som vi ska se, heltäckande.

Till större delen är det privata aktörer som äger den tekniska infrastrukturen och sköter driften av Internet i Sverige. Den information som förmedlas via nätet har också vanligen privata avsändare och riktar sig till privata mottagare. Yttrande- och informationsfriheterna formuleras i TF och YGL som medborgarens skydd mot staten, inte som någon skyldighet för enskilda aktörer (till exempel Internetoperatörer) att vidarebefordra andra enskilda aktörers yttranden. Frågan är om det överhuvudtaget ska vara statens ansvar att säkra ett fritt informationsflöde på Internet? Låt oss återkomma till den frågan.

Tekniskt motiverad filtrering

Som redan påpekats har företag och organisationer som äger och underhåller de servrar som utgör Internets noder ett ansvar för att hela systemet fungerar, vilket i sig kan fordra att dataströmmar blockeras i vissa lägen och i viss utsträckning. Internetoperatörerna filtrerar kontinuerligt och i stor utsträckning skräppost, så kallad spam. Här är problemet att det inte finns någon given definition av skräppost. Reklamerbjudanden som mottagarna inte har förklarat sig villiga att ta emot är utan tvekan skräppost, men är massutskick

av politiska budskap det? De flesta skulle sannolikt svara ja, och kanske måste Internetoperatörerna gå på den linjen av praktiska skäl, men att filtrera politisk opinionsbildning borde i en demokrati rimligen inte få ske slentrianmässigt eller okontrollerat.

Att operatörerna filtrerar för att skydda Internet som tekniskt system är alltså nödvändigt men också problematiskt på flera sätt. I samband med större virusattacker kan filtrerandet intensifieras. Man kan välja att blockera till exempel en viss typ av filer som visat sig innehålla virus. Riskerna för att även ”oskyldigt” material därmed filtreras bort är uppenbara.

Formellt sker operatörernas tekniskt motiverade filtrering med kundens godkännande, eftersom det framgår av abonnemangsavtalen att de får vidta den sortens åtgärder när det är nödvändigt av säkerhetsskäl. Som i många andra sammanhang är det dock inte ett godkännande i full frihet. Det avtal som Internetoperatören erbjuder kunden är i praktiken inget förslag utan ensidigt dikterade villkor. Jag kan inte som enskild kund börja förhandla med en multinationell koncern i mediabranschen om hur mycket just min Internetuppkoppling ska filtreras.

Filtrering av barnpornografi i Sverige

Den enda större, organiserade satsningen på innehållsfiltrering i Sverige tar alltså sikte på webbplatser med kommersiell hantering av barnpornografi. Gruppen mot sexuella övergrepp mot barn på Rikskriminalpolisen i Stockholm tar emot tips om sådana webbplatser och tittar närmare på dem.[86] Tipsen kommer från andra polismyndigheter, från allmänheten eller från barnrättsorganisationen Ecpats hotline/larmcentral. (Ecpat står för End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes.) Vid Rikskriminalpolisen gör man en bedömning av om materialet utgör barnpornografi i rättslig mening, och om så är fallet meddelar

86 http://www.polisen.se/Om-polisen/Sa-arbetar-Polisen/Om-olika-brott/Sexuella-overgrepp-mot-barn-och-barnpornografi/

man ett dussintal svenska Internetleverantörer som har valt att medverka vilken webbplats som bör blockeras. Av polisens information framgår inte hur många adresser som finns på svarta listan. Alla Internetleverantörer är således inte med i samarbetet, men enligt Rikskriminalpolisen egen uppskattning filtrerar man bort barnporr för närmare 90 procent av de svenska Internetanvändarna.

Att man begränsar filtreringen till barnpornografi som sprids på kommersiella villkor, det vill säga att man inte försöker filtrera all barnpornografi, har främst praktiska orsaker. Högre ambitioner i bekämpningen av barnpornografi skulle fordra större resurser. Åtskilligt bildmaterial som sannolikt är olagligt återfinns på enskilda personers webbplatser utan kommersiellt syfte. Dessa webbplatser är många och instabila. De kan ha kort livslängd och innehållet ändras ofta. Barnpornografi sprids också via sammanslutningar (*communities*) som fordrar medlemsskap och lösenord av den som vill bli insläppt. Praktiskt taget all barnporr som svensk polis finner på Internet har sitt ursprung i andra länder, och det är vanligt att man kontaktar polis i ursprungslandet med information om att olagligt material sprids. Det sker oavsett om spridningen sker i kommersiell form eller inte. Barnpornografi är förbjuden i nästan alla länder, men hur stora polisiära ansträngningar som görs i kampen mot den varierar. Svensk polis har små möjligheter att följa upp om de egna tipsen leder till åtgärder på andra håll i världen.

Ett problem med den svenska modellen – liksom med bland annat den norska, danska och engelska – är att personer eller organisationer som anser sig orättvist utsatta för filtrering inte kan få sin sak rättsligt prövad. Rikskriminalpolisen skickar listor över svartlistade webbadresser till operatörerna, men fattar aldrig något formellt beslut som kan överklagas. Listornas innehåll är hemligt, vilket gör det omöjligt för utomstående att bedöma hur stor överblockeringen är. Operatörerna har formulerat sina avtal med kunderna så att filtreringen är tillåten. Den filtrerade är maktlös.

Har regering, domstolar eller andra myndigheter stöd i lag för att besluta om filtrering i Sverige?

Yttrandefrihet garanteras alltså genom både tryckfrihetsförordningen, TF, och yttrandefrihetsgrundlagen, YGL. Därutöver finns formuleringar i regeringsformen, RF, om medborgarnas rätt till yttrandefrihet och informationsfrihet. De senare bestämmelserna har enskilda i praktiken små möjligheter att åberopa i domstol, de kan snarast beskrivas som instruktioner till riksdagen om hur den får stifta vanlig lag.

TF:s och YGL:s bestämmelser handlar om mer än enbart rätten att yttra sig. Regelverken hindrar i princip myndigheterna från att någonstans försvåra den process som ska leda till att grundlagsskyddade yttranden blir till. TF:s skydd täcker alltså skribentens insamlande av information, bearbetande av insamlat material, skrivande, sättning, tryckning och distribution till platser för utdelande/försäljning av tryckta skrifter. (Av praktiska skäl är YGL:s skydd inte fullt lika heltäckande, men skillnaderna mellan TF:s skydd och YGL:s behöver inte utredas här.)

TF:s regler kan åberopas som skydd för spridning av information via Internet bara när en periodisk skrift sprider sitt material också i form av en ”utsändning” – som ett kontinuerligt flöde av information på till exempel webbplatsen som mottagaren inte kan påverka. Det följer av den så kallade bilageregeln i TF 1 kap. 7 §.[87]

Yttrandefrihetsgrundlagen, YGL, ger alltså radio- och teveprogram, videoband och liknande ”tekniska upptagningar” samma sorts skydd som TF ger tryckta skrifter. Yttranden som görs tillgängliga för allmänheten i form av ljud- eller bildupptagningar

87 Länge levde åtminstone tidningsbranschen i föreställningen att en periodisk skrift som spred sitt material också via en databas på nätet – en databas ur vilken enskilda via Internet valde artiklar – kunde åberopa bilageregeln. Ett avgörande i Högsta Domstolen 2003 (NJA 2003 sid 31) tyder dock på att det istället är den så kallade databasregeln i yttrandefrihetsgrundlagen (YGL 1 kap 9 §) som då ska tillämpas. Databasregeln gäller således dels när ett etablerat medieföretag väljer att sprida information via Internet på ett sådant sätt att den är sökbar, oavsett om samma material också sprids via tryckt skrift, dels när enskilda eller organisationer har skaffat utgivningsbevis från Radio- och teveverket för till exempel en webbsida.

som bara kan uppfattas med något tekniskt hjälpmedel kan alltså få grundlagsskydd. Upptagningen ska då vara försedd med uppgift om ansvarig utgivare och kopia av den ska sparas för att det i efterhand inte ska råda något tvivel om vad som egentligen yttrades. Detta betyder att även webbplatser numera kan få grundlagsskydd. För etablerade medieföretag till exempel, som sprider nyheter och annat journalistiskt material på flera sätt, gäller lika starkt skydd oavsett om publicering sker i en papperstidning eller på webbplatsen.

Personer eller organisationer som vill ha grundlagsskydd när de sprider information via Internet kan få det genom att betala 2 000 kronor för ett så kallat utgivningsbevis från Radio- och teveverket, en statlig myndighet. Eftersom den ansvarige utgivaren måste kunna bestämma innehållet på webbplatsen kan dock inte alla former för informationsspridning via Internet få grundlagens skydd. När besökarna kan skriva in något eller på annat sätt förändra en webbplats innehåll – som på ett chatforum eller när en bloggare öppnar för kommentarer – blir grundlagsskydd uteslutet.[88]

”Myndighetsbeslut om filtrering som hindrar eller försvårar spridandet av grundlagsskyddade yttranden är dock förbjudna, åtminstone när beslutet syftar till att hindra spridning av visst innehåll.”

Att informationsfrihet råder stadgas alltså i Regeringsformen, RF, (2 kap 1 § 2 p) och definieras som *frihet att inhämta och mottaga upplysningar samt i övrigt taga del av andras yttranden*. Informationsfriheten får emellertid inskränkas genom vanlig lag (RF 2 kap 12 § och 13 §). Det betyder att en myndighet kan vidta åtgärder som leder till att *icke grundlagsskyddade* yttranden stoppas – den kan utöva förhandscensur – under förutsättning att den har stöd för det i lag.

Myndighetsbeslut om filtrering som hindrar eller försvårar spridandet av *grundlagsskyddade* yttranden är dock förbjudna, åtminstone när beslutet syftar till att hindra spridning av visst innehåll (YGL 1 kap 3 §). Om ett beslut om filtrering däremot kan motiveras med säkerhetsargument – om till exempel en myndighet beordrar operatörerna att filtrera med hänvisning till att Internet som tekniskt system annars kunde skadas – kan det vara lagligt. Man kan jämföra med att polisen inte får hindra någon att sälja en viss tidning, men att den av säkerhetsskäl får hindra personer från att sälja tidningar överhuvudtaget *på en viss plats*, på motorvägen till exempel.

88 För detaljer om utgivningsbevis och dess villkor, se: http://www.rtvv.se/se/Internet/

TF förbjuder förhandscensur. Ingripanden mot brottsliga yttranden får enligt TF och YGL alltså bara ske i efterhand. Att på en myndighets order eller initiativ filtrera bort yttranden så att de inte kan nå mottagare vore knappast förenligt med detta förbud mot *i förväg lagda hinder* för spridning. Det spelar ingen roll hur säker man är på att det man filtrerar bort är yttrandefrihetsbrott.

Fattas idag myndighetsbeslut om filtrering som tar sikte på innehåll? Formellt nej, i praktiken ja. Rikspolisstyrelsen är med i beslutsprocessen när det gäller barnpornografi, men den filtreringen blir inte ett problem enligt TF eller YGL eftersom grundlagarsreglerna överhuvudtaget inte ska tillämpas på just barnpornografi (TF 1 kap 10§ och YGL 1 kap 13§). Om man vill ägna sig åt konstitutionell djupanalys kan man fråga sig om inte filtrering av barnpornografi fordrar uttryckligt lagstöd för att vara förenlig med RF:s garantier för informationsfriheten (RF 2 kap 1§ p 2). Den frågan diskuterades inte när förbudet mot innehav av barnpornografi infördes, (brottsbalken 16 kap § 10 a), men att ett förbud mot innehav av information kan anses utgöra ett förbud även mot att avsiktligt ta emot den förefaller rimligt. Inte heller RF skulle därmed utgöra något hinder mot myndigheters beslut om filtrering av barnpornografi. Just barnpornografi blir dock ett specialfall eftersom innehavsförbud inte gäller för någon annan typ av information. Bara där har en möjlighet till förhandscensur öppnats.

Två villkor för att myndighetsbeslut om innehållsfiltrering av Internet ska vara tillåtna i Sverige är alltså (1) att inte grundlagsskyddade yttranden blockeras, och (2) att det föreligger lagstöd. En tredje fråga blir, om de båda första villkoren är uppfyllda, i vilken utsträckning överblockering kan tillåtas? Överblockering som drabbar grundlagsskyddat material torde inte kunna accepteras överhuvudtaget. Om – eller när – riksdagen med lagstiftning öppnar möjlighet till statligt beslutad filtrering måste den frågan utredas närmare. De olika metoderna för filtrering kan, som tidigare påpekats, ge högst olika effekter i form av under- och överblockering.

Självsanering – rättsligt stöd för Internetoperatörers beslut om filtrering i Sverige

Internet domineras av privata aktörer. Företag äger merparten av de fysiska ledningarna och datorerna och sköter driften i flertalet av de noder som får hela systemet att fungera.

Dessa privata handhavare av Internet är inte bundna av grundlagens garantier för yttrande- och informationsfriheterna. Med högst varierade motiv begränsar eller blockerar de i själva verket åtskilligt i nätets informationsflöden. Säkerhets- och funktionalitetsmotiven är starka. Virus och annan destruktiv programkod hotar, liksom skräppost, att skada Internet som kommunikationssystem. Av lagen (2003:89) om elektronisk kommunikation, LEK, framgår att de operatörer som tillhandahåller allmänna kommunikationsnät har skyldighet att i olika avseenden säkra driften.

För att skydda kundernas integritet är operatören dock förbjuden att *behandla* kunders elektroniska meddelanden utan deras samtycke (LEK 6 kap 17 §). Följaktligen har de företag som erbjuder Internetuppkoppling normalt sett till att i avtalen med kunderna tillförsäkra sig långtgående rättigheter att *behandla* – att blockera informationsströmmar, stänga av webbsidor och avsluta abonnemang. Det förekommer alltså att operatörerna med åberopande av innehållet i privata avtal stänger av kunder som inte misstänks för någon brottslighet. Enligt författarens bredbandsavtal med Telia från 2003 kan tjänsten stängas av flera skäl varav de flesta hänvisar till situationer där användaren gör något som kan skada eller störa Internets tekniska funktioner. Det kan dock enligt avtalsvillkoren räcka med att *”avsevärda olägenheter uppstår för Telia eller annan”*. Någon precisering av begreppet *olägenhet* finns inte i avtalet och vad som är *avsevärt* kan naturligtvis alltid diskuteras.

”Med detta följer en skyldighet för operatören att ingripa om kunden missköter sig på något sätt som kan skada systemet.”

För operatörerna är filtrering ett nödvändigt ont. Internetoperatören säljer ju på sätt och vis mer än företaget har. Att ansluta en kund till Internet innebär att man ger kunden tillträde till alla andra Internetanslutna datorer i världen, inte bara till de som finns i den svenska operatörens eget nät. Med detta följer en skyldighet för operatören att ingripa om kunden missköter sig på något sätt som kan skada

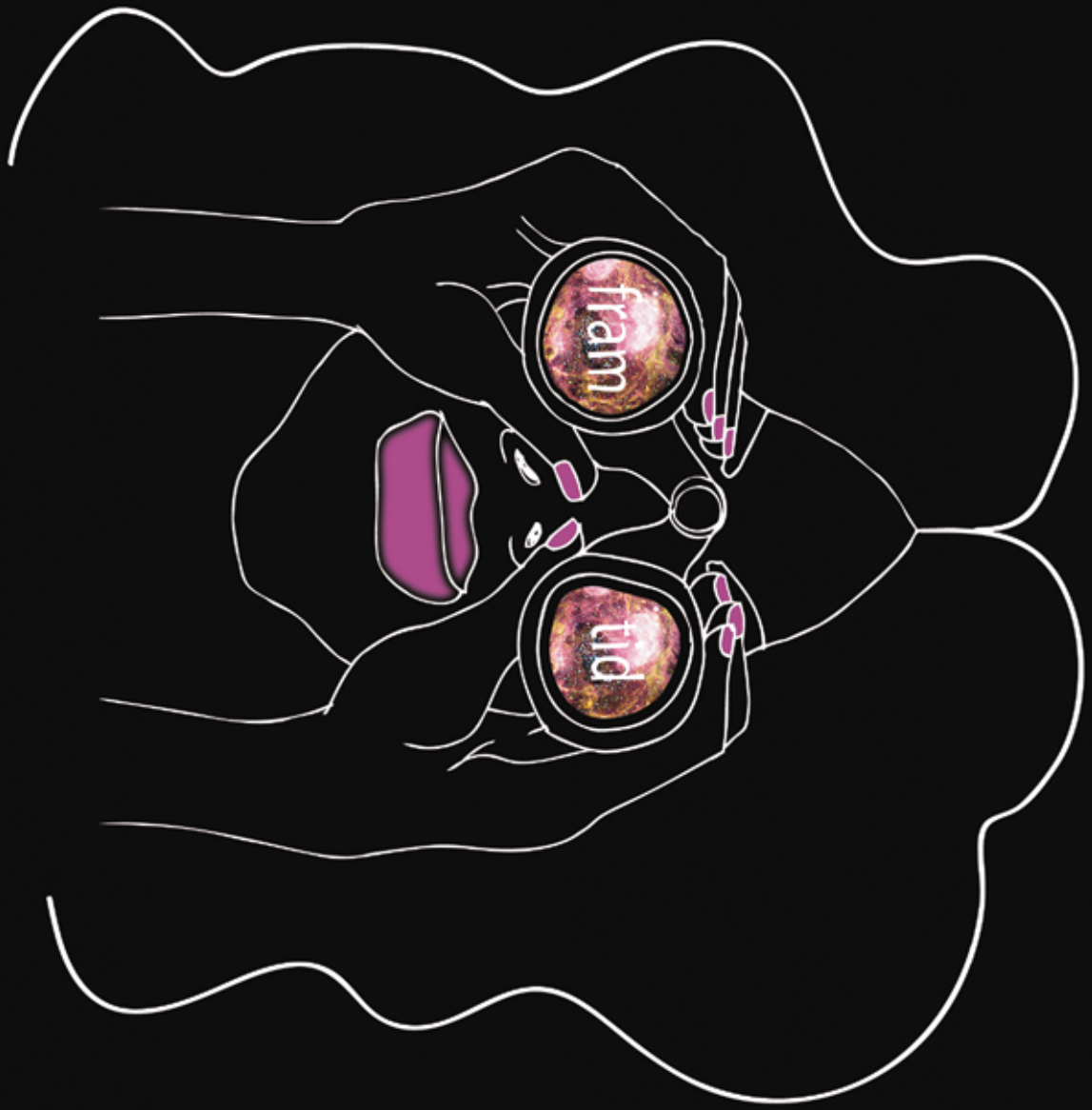
systemet. Är operatören i Sverige alltför passiv när det gäller att hålla efter kunder som skadar det tekniska systemet kan övriga Internetleverantörer i världen reagera och i värsta fall stänga den svenska operatören ute. I den meningen tvingas alla Internetoperatörer ta ett ansvar för hur kunderna beter sig, och stänga av dem som beter sig alltför illa.

Barnpornografin har ända sedan Internet blev en allmänt tillgänglig kommunikationskanal vållat de mest upprörda känslorna i Sverige och gett upphov till de mest drastiska ingripandena. Redan vid mitten av 1990-talet började Telia stänga av många så kallade nyhetsgrupper där företaget ansåg sig ha anledning att misstänka spridning av barnporr. Senare har andra operatörer valt att följa efter.[89] Det är ingen tvekan om att man samtidigt har stoppat material av helt annat slag, även om det är svårt att bedöma hur stor överblockeringen har varit.

Internetbranschens företag drar alltså inte någon principiell gräns mellan kunder som missköter sig så att nätdriften kan skadas och sådana som missköter sig på annat sätt. Även kunder som via Internet hotar eller kränker andra människor kan stängas av. Man gör då ingen juridisk bedömning av hotet eller kränkningen, det vill säga man uttalar sig inte om huruvida yttrandena utgör till exempel *olaga hot* eller *förtal* i lagens mening. Istället gör man en egen moralisk bedömning, vilket man skapat utrymme för med allmänt hållna formuleringar i avtalen. Det blir problematiskt ur yttrande- och informationsfrihetssynpunkt. Visserligen kan man hänvisa till att det finns få exempel på kontroverser kring Internetoperatörers ingripanden i detta avseende, men det tycks inte heller finnas några studier av hur stort problemet egentligen är.

89 *Internetoperatörer stoppar barnporr*. Svenska Dagbladet 2002-10-11.

Illustration: © Camilla Laghammar



Framtiden

Avslutningsvis några reflektioner för att knyta ihop resonemangen i tidigare kapitel.

Det enda som med någorlunda säkerhet kan sägas om filtrering i framtiden är att vi får politiska strider om saken, precis som vi har fått – och får – om de flesta andra åtgärder för skärpt kontroll över Internet.

Att hålla ett öga på utvecklingen i USA brukar vara en god idé, eftersom de flesta viktiga strider först blossar upp där. Tidningen ETC rapporterade på hösten 2009:

"I maj konstaterade USA:s president Barack Obama att regeringen inte är tillräckligt förberedd på att hantera störningar i den digitala infrastrukturen och meddelade att en ny tjänst som cybersäkerhetskoordinator skulle skapas inom Vita Huset. Ungefär samtidigt presenterades det första utkastet till en ny cybersäkerhetslagstiftning av senatorerna Jay Rockefeller och Olympia Snow. Det fick omgående hård kritik för att vara för långtgående i fråga om att ge Vita Huset makt över internet.

Texten har nu arbetats om, men det har inte lugnat många. Enligt förslaget ska presidenten kunna deklarera en 'cybersecurity emergency', det vill säga ett slags undantagstillstånd som ger administrationen rätt att vidta kraftfulla åtgärder för att bekämpa till exempel terrorism. Bland annat ska stora delar av internet kunna stängas ner för privata användare, skriver Cnet.com.

En annan del av förslaget är att vissa datasystem och nätverk i den privata sektorn måste administreras av licensierade 'cybersäkerhetsproffs', som har genomgått ett nationellt certifieringsprogram."[90]

En nyckelfråga är hur man ska definiera statens ansvar för systemet. Kan man hävda (som Obama-regeringen gör) att staten har ett övergripande ansvar för att Internet fungerar och samtidigt driva linjen att det *inte* är en statlig uppgift att garantera att medborgarna kan realisera sin yttrandefrihet där?

90 http://www.etc.se/23386/obama-ska-kunna-staenga-internet/

Mer specifikt om filtrering: Är det ett yttrande- eller informationsfrihetsproblem om en Internetoperatör med stöd i avtalet med kunden filtrerar bort information?

Ett möjligt svar är påpekandet att den kund som är missnöjd med hur hans/hennes Internetleverantör handskas med informationsströmmarna kan vända sig till en annan operatör. Privatpersoner har trots allt flera påfartsvägar till Internet, och så länge kunderna har rimliga möjligheter att informera sig om olika Internetleverantörers policy vad gäller filtrering bör marknadskrafterna få verka. Tillsynsmyndigheten Post & Telestyrelsen, PTS, kräver i en rundskrivelse till svenska operatörer 2004-12-08 att de måste klargöra för kunderna när och hur e-post filtreras. Om så inte sker kan kunderna heller inte anses ha samtyckt till att operatören raderar elektroniska meddelanden adresserade till dem.[91]

"Så länge det finns öppenhet och valmöjligheter i systemet kanske staten inte bör lägga sig i? Det är ingen orimlig ståndpunkt."

Så länge det finns öppenhet och valmöjligheter i systemet kanske staten inte bör lägga sig i?

Det är ingen orimlig ståndpunkt. Men man kan också, som författaren till denna guide, hävda att den utvägen är alltför enkel. Hur systemet fungerar idag, till exempel hur Internetoperatörerna utnyttjar sina möjligheter att tillrättavisa eller stänga av kunder, vet ingen. Det saknas studier i ämnet. Sådana behövs, men oavsett vad sådana kan visa finns det starka argument för att staten behöver ta ett visst ansvar för yttrande- och informationsfriheten på Internet. Alla aktörer (medborgare, företag, myndigheter) behöver garantier för att informationen verkligen kan flöda fritt i den tekniska infrastruktur som har central – och hela tiden växande – betydelse för samhällets utveckling i kommersiellt, socialt och demokratiskt avseende.

Lagstiftaren har på en principiell nivå konstaterat att problemet finns. I inledningsparagrafen i lagen om elektronisk kommunikation heter det:

"Vid lagens tillämpning ska skall särskilt beaktas elektroniska tjänsters betydelse för yttrandefrihet och informationsfrihet." (LEK 1 kap, 1 §, 3 st)

Å andra sidan konstateras i samma lag, något motsägelsefullt, att:

91 PTS ref nr 04-15500.

”Lagen är inte tillämplig på innehåll som överförs i elektroniska kommunikationsnät med hjälp av elektroniska kommunikationstjänster.” (LEK 1 kap, 4 § 2 st)

Det är knappast heller inom ramen för LEK som frågan bör få sitt svar. Av tradition skyddas i Sverige yttrande- och informationsfriheterna med grundlagsbestämmelser.

Det problem som uppstår när många svenska Internetoperatörer filtrerar webbplatser baserade i utlandet kan ”marknaden” möjligen anses lösa. Så länge det finns några operatörer i Sverige som inte filtrerar har kunderna åtminstone i teorin tillgång till ett ocensurerat Internet. (Man kan förstås fråga sig om det är rimligt att man måste bli kund hos en liten, resurssvag operatör med anarkistisk eller annan kontroversiell profil för att slippa censur, men den diskussionen ska inte fördjupas här.) Observera att vi då talar om informationsmottagarens problem, inte om avsändarens.

En svensk som via webben vill sprida ett lagligt men kontroversiellt budskap kan normalt (om inte annat utomlands) hitta en Internetleverantör som går med på att hysa webbsidan, men vilket värde har det om de större svenska Internetleverantörerna sedan filtrerar bort den? En medborgerlig rätt att slippa få sina yttranden filtrerade framstår som rimlig. Som ett minimum borde en sådan rätt avse webbsidor med grundlagsskyddat innehåll, men att begränsa rätten till TF:s och YGL:s områden är inte självklart.[92]

Som påpekats ovan har Europadomstolen i åtminstone ett fall, *Özgür Gündem mot Turkiet* från 2000, tolkat artikel 10 i Europakonventionen som en positiv förpliktelse för staten att hindra privata aktörer från att kränka andras yttrandefrihet. En statlig förpliktelse att säkra fria informationsflöden på Internet – lagstiftning med tydligt angivande av när blockering kan godtas – är mot den bakgrunden ett demokratiskt välgrundat krav.

92 Just denna diskussion kompliceras år 2010 av att en statlig utredning – Yttrandefrihetskommittén – arbetar med att ersätta den sedan länge gällande grundlagskonstruktionen till skydd för yttrandefriheten (baserad på TF och YGL) med något helt annat. Skulle kommittén föreslå att TF/YGL avskaffas till förmån för en annan sorts regelverk kan ett sådant, om riksdagen så beslutar, träda i kraft tidigast efter valet 2014.

Att som idag placera ansvaret för beslut om filtrering hos nätoperatörer innebär att dessa företag hamnar i konfliktsituationer som de i egenskap av aktörer på en fri marknad får svårt att hantera – situationer som de av demokratiskäl inte *bör* försättas i. När de större företagen i branschen 2005 tog beslutet att filtrera barnpornografi kunde det från moraliska utgångspunkter framstå som väl motiverat, men det var också ett principiellt beslut om att ta ansvar för vad kunderna får och inte får se. Företagen kan sedan dess inte avvisa krav på filtrering av annat stötande material med argumentet att ”Vi håller bara med det tekniska systemet. Vilken information människor kommunicerar där lägger vi oss inte i.” Beslutet att filtrera barnporr var kommersiellt grundat. Oavsett vilket företagsledningarna fruktade mest – att det egna företaget skulle bli utpekat som pedofilins försvarare eller att dess verksamhet kunde komma att skadas av det lagförslag Bodström hotade med – var det företagets bästa man hade för ögonen.

Om Internetleverantörerna ska bestämma vilken information och vilka åsikter som ska släppas fram på nätet får de också ett ansvar för yttrande- och informationsfriheten. Det är uppenbart olämpligt att sådant ansvar överlåts på aktörer som ena dagen kan ha starka ekonomiska incitament att värna friheterna, men nästa dag kan ha lika starka incitament att inskränka dem.

Att maximera medborgarnas yttrande- och informationsfrihet kan för styrelsen och Vd inte – åtminstone inte i längden – väga tyngre än företagets resultat och konkurrensförmåga. Internetoperatörens intresse av vinst och medborgarnas intresse av yttrandefrihet kolliderar kanske inte ofta, men det händer. Därför behövs lagstiftning som tydligt begränsar möjligheterna till filtrering.

Filter och demokrati

Det som kallas informationssamhället framstår som paradoxalt. Det tycks stå både för befrielse av människor och rikedom på information, men också för en hårdnande kamp om information – nämligen den information på vilken samhällelig kontroll eller in-

komster/försörjning kan baseras. Samhällelig kontroll kan den centralmakt utöva som har långtgående rättigheter att övervaka och registrera medborgarna, samtidigt som medborgarna har små möjligheter till insyn i detta övervakande och detta registrerande. I Sverige har det förra realiserats genom FRA-lagen och en rad andra nya/förstärkta tvångsmedel och det senare genom kraftiga inskränkningar i offentlighetsprincipen.[93] Inkomster genereras – vanligen små för individer men stora för företag – för dem som kan göra anspråk på upphovsrätt, patent och andra så kallade immateriella rättigheter.

”Precis som i alla andra epoker måste de organisera sig … och ta strid för att få inflytande och för att säkra fri- och rättigheter värda namnet.”

Denna kamp om kontrollen över information och informationsflöden kan medborgarna inte ställa sig utanför. Precis som i alla andra epoker måste de organisera sig (i någon mening) och ta strid för att få inflytande och för att säkra fri- och rättigheter värda namnet. Ur det perspektivet är föreställningarna om Internet som en ”fri” eller ”okontrollerbar” värld direkt skadliga för demokratin. De har inte bara dålig täckning i verkligheten, de fungerar passiviserande snarare än aktiverande. Varför ta strid mot statlig kontroll över Internet om Internet ändå är okontrollerbart?

Den brittiske medieforskaren Brian Winston publicerade 1998 en bok där han hävdar att de historiska erfarenheterna är så entydiga att man kan tala om en ”lag” i utvecklingen av kommunikationsteknologier – *”the law of the suppression of radical potential”* (ungefär: Lagen om undertryckande av radikal potential).[94]

Han visar med historiska exempel – från telegrafen till Internet – hur de ekonomiskt och politiskt starkaste skikten i varje samhälle självklart, som vore det en naturlag, undertrycker de möjligheter till maktförskjutning som nya kommunikationsteknologier skapar. I Winstons resonemang ligger inte något konspirationstänkande. Typiskt sett anser alla de institutioner, sociala skikt och individer som redan *har* ett stort inflytande över samhällsutvecklingen att denna maktposition är berättigad. Lika självklart är det därför att de hela tiden, närmast instinktivt, arbetar på att försvara och be-

93 För en genomgång av de senaste 30 årens inskränkningar i offentlighetsprincipen, se: Olsson, Anders R: *Att stänga det öppna samhället*. Tusculum Förlag 2008.

94 Winston, Brian. *Media and Technology. A history: From the Telegraph to the Internet.* Routledge 1998.

fästa den. Det vore ju märkligt om de, enbart på grund av något steg i kommunikationsteknologiernas utveckling, frivilligt skulle avhända sig möjligheter till inflytande.

En möjlighet att utöva inflytande på Internet är alltså filtrering. Den, liksom övriga möjligheter, behöver studeras och diskuteras. Och det bör inte ske en fråga i taget, när en plötsligt uppblossande opinionsstorm i gamla eller nya medier så kräver. Det bör ske med helheten för ögonen och med vårt behov av yttrande- och informationsfrihet som utgångspunkt.

”En möjlighet att utöva inflytande på Internet är alltså filtrering. Den, liksom övriga möjligheter, behöver studeras och diskuteras. Och det bör inte ske en fråga i taget, när en plötsligt upplossande opinionsstorm i gamla eller nya medier så kräver. Det bör ske med helheten för ögonen och med vårt behov av yttrande- och informationsfrihet som utgångspunkt.”

.SE (Stiftelsen för Internetinfrastruktur) är en oberoende allmännyttig organisation som verkar för en positiv utveckling av Internet i Sverige. Utöver att ansvara för Internets svenska toppdomän bedriver .SE ett omfattande utvecklingsarbete:

- **.SE:s Internetguider** är en skriftserie som riktar sig till intresserade lekmannaanvändare och behandlar olika Internetfrågor. Denna publikation ingår i serien. Läs mer: iis.se/se-ar-mer/ses-publikationer.
- **Webbstjärnan** är en tävling i webbpublicering för skolan. Syftet är att dra nytta av Internets möjligheter i skolarbetet, genom att bygga en webbplats kring ett valfritt skolarbete. Läs mer: webbstjärnan.se och stjärnkikarna.se.
- **Internet för alla.** .SE bidrar till olika åtgärder för att förbättra tillgängligheten till Internet för de grupper som idag inte är anslutna till nätet.
- **Pålitlig e-post**. .SE undersöker vad som kan göras för att öka säkerheten och förtroendet för e-post för både företag och privatpersoner.
- **IPv6 och DNSSEC** är två viktiga teknikprojekt som ska säkerställa att Internets infrastruktur även i fortsättningen kan vidareutvecklas och fungera säkert. Läs mer: ipv6forum.se respektive iis.se/domaner/dnssec/.
- **Bredbandskollen** är ett konsumentverktyg som hjälper bredbandskunder att utvärdera sin bredbandsuppkoppling. Läs mer: bredbandskollen.se
- **Internetstatistik** .SE har tagit initiativ för att etablera ett samarbete kring statistik och fakta om Internet, vilket bland annat resulterat i den tryckta rapporten Svenskarna och Internet. Läs mer: iis.se/se-ar-mer/ses-publikationer och internetstatistik.se.
- **Internetfonden** bidrar till Internetutvecklingen genom att finansiera fristående projekt. Bland uppdragstagarna finns organisationer, privatpersoner och akademiska institutioner. Läs mer: iis.se/se-ar-mer/internetfonden.
- **Internetdagarna** är .SE:s årligen återkommande konferens för alla som arbetar med Internet. Läs mer: internetdagarna.se

.se

Som en del i .SE:s arbete med Internetutveckling producerar .SE ett antal skrifter under produktnamnet .SE:s Internetguider. Guiderna behandlar olika Internetrelaterade områden och riktar sig i första hand till intresserade lekmannaanvändare. En guide kan vara såväl en praktisk handbok som en mer beskrivande rapport.

.se
Stiftelsen för Internetinfrastruktur