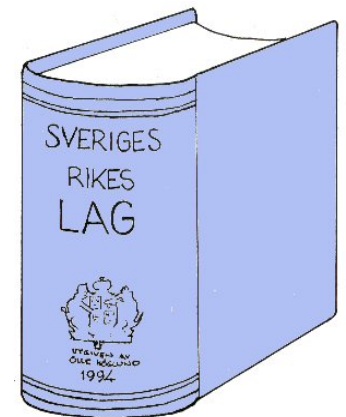


IT-(o)säkerhet och Juridik

Conny Larsson & André Rickardsson



När din IP-adress eller dina
personuppgifter återfinns i en logg
är du skyldig

Ovanstående gäller i synnerhet
om du är en man

IT-säkerhet är en illusion

**Alla datorprogram med mer än 100
rader kod har brister**

IT-säkerhet är en illusion

- Ett mycket bra skydd av WLAN enligt PTS
 - IEEE 802.11i
 - AES krypto
 - Lång nyckel > 16 tecken
 - Alfamerisk
 - Stora små bokstäver
 - VPN
 - Osv.

WPA2 och IEEE 802.11i anses vara mycket säkert. Det finns idag inga kända metoder för att attackera WPA2, Källa (PTS)

Slå på krypteringen

Du bör slå på routerns inbyggda krypteringsfunktion. Det finns idag tre olika krypteringar – WEP, WPA och WPA2. Den svagaste krypteringen är WEP. Den är relativt lätt att knäcka, men skyddar mot spontan avlyssning. WPA är betydligt säkrare än WEP, men inte lika bra som WPA2 – den starkaste krypteringen. WPA2 ger ett mycket bra skydd.

Källa: <http://www.pts.se/sv/Internet/Internetsakerhet/For-hemmet/Ansluta-tradlost-hemma/Hur-skyddar-jag-mig/>

IT-säkerhet är en illusion

DEMO

Gone in 60 seconds

IT-säkerhet är en illusion

- Har inte attackerat krypteringen
- Utnyttjar en säkerhetsbrist i implementationen
- Ingen kryptering eller autentisering sker av kontrolltrafik mellan klienten och accesspunkten
- Inget fel på WPA2 men är WLAN säkert 😊

WPA2 och IEEE 802.11i anses vara mycket säkert. Det finns idag inga kända metoder för att attackera WPA2,
Källa (PTS)

IT-säkerhet är en illusion

- IT-osäkerhet och Juridik
- Vad har detta för konsekvenser för
 - Lagstiftning
 - Avtal
 - Bevissäkring
 - Beviskrav & bevisvärdering

Rättskällor

- 
- 1992** – *Datastraffrättsutredningen (SOU 1992:110)*; Uppmärksammar bl.a. om att vissa IT-brott inte omfattas
 - 2001** – *Convention on Cybercrime (ETS no.: 185)*; Lagharmonisering med krav på vissa nationella regler
 - 2002** – *Utkast Rambeslut (EGT C203E, 27/8 2002)*; EU-beslut om nationella regler med CCC som förebild
 - 2002** – Justitiedep:s uppdrag att behandla frågan om Sveriges tillträde till/implementering av CCC, 20/12 2002
 - 2003** – *Tilläggsprotokoll (ETS no.: 189, 28/1 2003)*; Komplettering avseende rasism och främlingsfientlighet
 - 2003** – Ökad effektivitet och rättssäkerhet i brottsbekämpningen – preventiva åtgärder mm (SOU 2003:74)
 - 2004** – *Förslag att riksdagen skall godkänna förslaget till rambeslut (Prop. 2003/04:164)*; - Vissa kompletteringar återstår i lagreglerna, Riksdagen godkände rambeslutet 27/10 2004
 - 2005** – *Rambeslut (2005/222/RIF, 24/2 2005)*; Rådet antar EU-beslut om nationella regler med CCC som förebild
 - 2005** – *Angrepp mot informationssystem (Ds 2005:5)*; Förslag till nödvändiga lagändringar
 - 2005** – *Brott och brottsutredning i IT-miljö (Ds 2005:6)*; Slutligt betänkande
 - 2005** – Elektronisk kommunikation i brottsutredningar (SOU 2005:38)
 - 2007** – *Angrepp mot informationssystem (Prop. 2006/07:66)*; Utvidgning i BrB 4:9c, ikraft 1/7 2007

(t)

Cyber Crime Convention



Convention on Cyber Crime

ETS no 185

(Europarådets konvention om IT-relaterad brottslighet)

- Antogs av Ministerrådet 8/11 2001
- Trädde i kraft 1/7 2004

Sverige har skrivit på:

- Konventionen, 23/11 -01
 - tilläggsprotokoll, 28/1 -03
- men ännu ej ratificerat!

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access (Olagligt intrång i datorsystem)

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception (Olovlig avlyssning av datorbehandlingsbara uppgifter och av elektromagnetiska emissioner från datorer och datorsystem)

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference (Datastörning)

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference (Systemstörning)

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

BrB 4 kap

BrB 4 kap

8 § Den som olovligen bereder sig tillgång till ett meddelande, som ett post- eller telebefordrings-företag förmedlar som postförsändelse eller telemeddelande, döms för **brytande av post- eller telehemlighet** till böter eller fängelse i högst två år.

(Lag 1993:601).

9 § Den som, utan att fall är för handen som i 8 § sägs, olovligen bryter brev eller telegram eller eljest bereder sig tillgång till något som förvaras förseglat eller under lås eller eljest tillslutet, dömes för **intrång i förvar** till böter eller fängelse i högst två år.

9 a § Den som i annat fall än som sägs i 8 § olovligen medelst tekniskt hjälpmedel för återgivning av ljud i hemlighet avlyssnar eller upptager tal i enrum, samtal mellan andra eller förhandlingar vid sammanträde eller annan sammankomst, vartill allmänheten icke äger tillträde och som han själv icke deltar i eller som han obehörigen berett sig tillträde till, dömes för **olovlig avlyssning** till böter eller fängelse i högst två år.

Lag (1975:239).

9 b § Om någon anbringat tekniskt hjälpmedel med uppsåt att bryta telehemlighet på sätt som sägs i 8 § eller att utföra brott som sägs i 9 a §, dömes för **förberedelse** till sådant brott till böter eller fängelse i högst två år, om han ej är förfallen till ansvar för fullbordat brott.

Lag (1975:239).

9 c § Den som i annat fall än som sägs i 8 och 9 §§ olovligen bereder sig tillgång till **en uppgift som är avsedd för** automatisk databehandling eller olovligen ändrar eller utplånar eller i register för in **en sådan uppgift** döms för **dataintrång** till böter eller fängelse i högst två år. **Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift.**

Lag (1998:206).

Och ändrad genom lag (2007:213).

Borde inte reglerna om "informationsintrång" gälla lika oberoende av teknik?

Informationen har väl samma värde oavsett "förpackning"?

Finns det någon anledning att behandla information olika beroende på vilket medium som har använts?

Därmed borde väl dessa regler kunna sammanföras till en enda – eller...?

Ändring BrB 4:9c

Angrepp mot informationssystem

(Ds 2005:5 och prop. 2006/07:66)

- Syftar till att genomföra EU:s rambeslut om angrepp mot informationssystem
- Därför krävs ett utvidgat straffansvar i förhållande till gällande rätt på området
- Utvidgningen föreslås ske i bestämmelsen om dataintrång i brottsbalken (4:9 c)
 - dels att omfatta den som olovligen blockerar en uppgift som är avsedd för automatiserad behandling,
 - dels den som olovligen allvarligt stör eller hindrar användningen av en sådan uppgift
 - även försök och förberedelse till sådana brott straffbeläggs
 - medverkan till sådana brott blir också straffbart
- Kriminaliseringen innebär exempelvis att s.k. tillgänglighetsattacker blir straffbara (som sker t ex genom datavirus och DOS-attacker)
- Vidare förtydligas dataintrångsbestämmelsen och moderniseras språkligt genom att uttrycket "uppgift som är avsedd för automatiserad behandling" ersätter det tidigare använda upptagningsbegreppet
- Infördes i BrB 4:9c genom lag (2007:213), som trädde ikraft 1/7 2007



Återstår

Ändringen i 4:9c

BrB 4 kap 9 c § Den som i annat fall än som sägs i 8 och 9 §§ olovligen bereder sig tillgång till *en uppgift som är avsedd för automatisk databehandling* eller olovligen ändrar eller utplånar eller i register för in *en sådan uppgift* döms för **dataintrång** till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift.

Detta medför att **datastörning och systemstörning (datavirus, DOS-attacker etc) blivit straffbara**

- Uppfyller helt eller delvis art 4 och 5 i CCC, jämte art 3 och 4 i Rambeslutet (jfr Ds 2005:6 s. 95 ff och 206)

Traditionellt dataintrång (och även brytande av telehemlighet) täcks redan av befintlig text

- Uppfyller art 2 i CCC, jämte art 2 i Rambeslutet (jfr Ds 2005:6 s. 93-95 ff och 205 f)

Förslaget i Ds 2005:6

BrB 4 kap 9 c § Den som i annat fall än som sägs i 8 och 9 §§ olovligen bereder sig tillgång till *upptagning för automatiserad databehandling* eller olovligen ändrar eller utplånar eller i register för in *en sådan upptagning eller med tekniskt hjälpmedel avlyssnar elektromagnetiska emissioner eller andra icke allmänt tillgängliga signaler till eller från en dator eller inom ett datorsystem i syfte att få del av information* döms för **dataintrång** till böter eller fängelse i högst två år. *Med upptagning avses härvid även uppgifter som är under befordran via elektroniskt eller annat liknande hjälpmedel för att användas för automatiserad informationsbehandling.*

Detta medför att **avlyssning av annan datortrafik jämte RÖS mm ännu inte blivit straffbara!**

- Återstår att uppfylla delar av art 3 i CCC (jfr Ds 2005:6 s. 95-97 och 208)



Tillämpa andra regler?



Kan alternativa straffbestämmelser tillämpas t ex mot datavirus, maskar, logiska bomber eller DOS-attacker? (jfr Ds 2005:6 s. 102 f)

- Skadegörelse (BrB 12:1)
 - långsökt, eftersom skadan inte är *fysisk*
- Sabotage (BrB 13:5)
 - osannolikt, eftersom det sällan drabbar "vitala samhällsintressen"
- Egenmäktigt förfarande (BrB 8:8)
 - knappast, då angreppsobjektet måste vara något med fysisk substans
 - jfr Stockholms TR, B 353-06: DOS-attack bedömd som egenmäktigt förfarande då det "rubbat annans besittning" till datorsystem

Ändringen i BrB 4:9c bör ha medfört att detta blivit straffbart som *datastörning* och *systemstörning* och att det därmed inte längre är intressant att försöka tillämpa andra bestämmelser...?

Radiotrafik

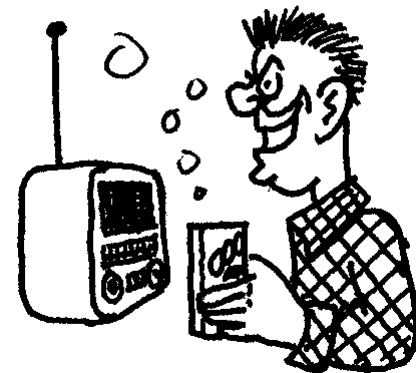
Vad gäller för information som förmedlas via radio?

(jfr Ds 2005:6 s. 93 och Ds 2005:5 s. 57 f)

- Radiomeddelanden faller utanför det straffbara området!
- Omfattas dock av en särskild tystnadsplikt! (LEK 6:23)
 - gäller inte bara teleoperatör utan även alla andra

(prop. 2002/03:110 s 397, som h v t prop.1992/93:200 s 311 f och 166 f)

- Hur kan man veta när en uppgift i detta allmänt tillgängliga media är hemligt!!!????



Hip hip hora-målet

Tingsrätten

- Igen kontroll sker av det viktigaste beviset en DVD-skivan som påstods innehålla den nedladdade filmen Hip Hip Hora
 - Ingen kontrollera DVD-skivan, inte polisen, åklagaren, domstolen eller advokaten
- Igen husrannsakan genomförs
- Det finns inget i anmälan eller utredningen som beskriver hur angivna datum, tider verifierats eller vilken tidszon det avser därför kan man inte kontrollera uppgiften med Bredbandsbolaget
- I polisförhöret med den åtalade omnämns överhuvudtaget inte utdelning av filer eller filmen Hip Hip Hora

Beviskrav & bevisvärdering

STÄLLT UTOM VARJE RIMLIGT TVIVEL!!!

- HD har dels fastslagit att detta beviskrav gäller!
- HD har även i flera domar fastslagit att lägre beviskrav inte får tillämpas bara för att bevisningen är krånglig!
- Det skall därmed kunna *uteslutas* att någon annan förklaring kan föreligga!

NJA 1980 s. 725 – beviskravet fastställs!

NJA 1982 s. 164 – narkotikamål

NJA 1982 s. 525 – våldtäktsmål

NJA 1959 s. 63

NJA 1970 s. 58

NJA 1980 s. 514

NJA 1980 s. 725

NJA 1982 s.114

NJA 1982 s. 164

NJA 1982 s. 525

NJA 1986 s. 821

NJA 1990 s. 210

NJA 1990 s. 555

NJA 1991 s. 83

NJA 1992 s. 446

NJA 1993 s. 86

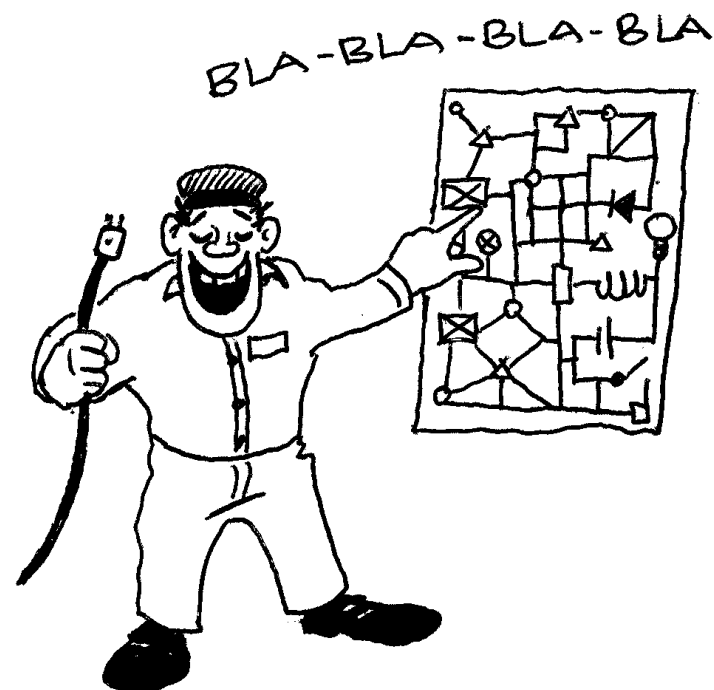
NJA 1993 s. 616

NJA 1996 s. 27

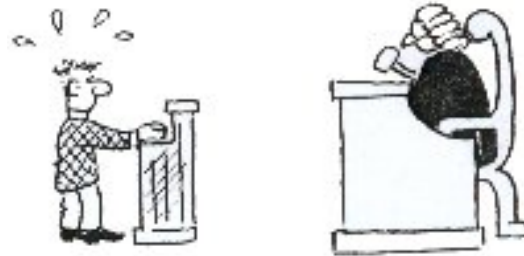
NJA 1996 s. 176

NJA 2002 s. 449

NJA 2004 s. 231



Rättspraxis – Hip hip hora-målet



Upphovsrättsintrång, fildelning mm:

För att kunna ådömas ansvar för den gärning som åklagaren har lagt den tilltalade till last krävs dels att det är styrkt att det IP-nummer som framgår av utredningen har tilldelats datorutrustning som tillhör eller disponerats av den tilltalade, dels att det kan uteslutas att någon annan använt sig av denna utrustning vid den angivna tidpunkten.

(Svea Hovrätt 2006-10-02, mål nr B 8799-05)

- ***Du måste inte bara styrka IP-adressen!***
- ***Du måste även kunna styrka att det inte kan vara någon annan!***

Säkerhetsfrågan

ÄR UPPGIFTERNA TILLFÖRLITLIGA?

Komplexitet

- Kan systemen/informationen förstås och kontrolleras?
- Större komplexitet = mindre tillförlitlighet!**

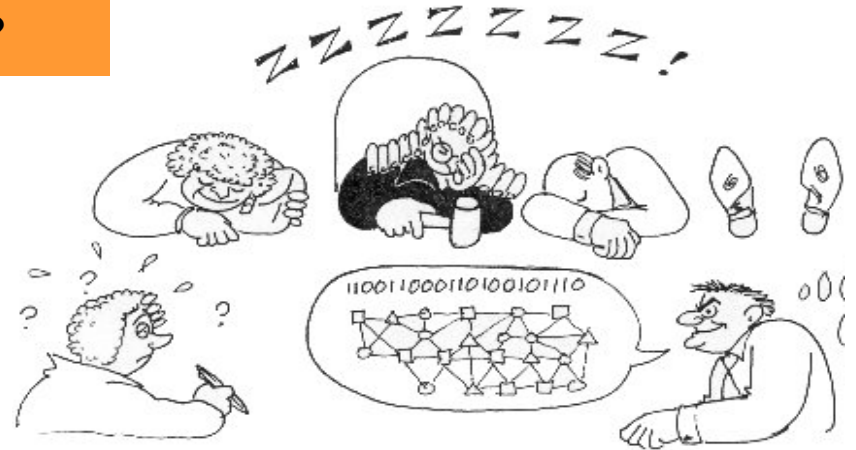
Kontroll

- Hur kontrollerar TO:s/ISP sina system?
- Mindre kontroll = mindre tillförlitlighet!**

Säkerhet

- Hur skyddas systemen/informationen?
- Störningar?
- Obehörig tillgång?

Sämre säkerhet = mindre tillförlitlighet!
D.v.s. lägre bevisvärde!!!



Olyckligtvis en sann bild från en svensk rättssal någon gång under 90-talet. Den åtalade dömdes till fängelse för (dator)bedrägeri. Visste verkligen domstolen vad de dömde?



Som jurister;

- Ifrågasätter vi informationen ordentligt?
- Vet vi vilka frågor vi skall ställa?

Blind tro på loggar

Litar utredare för mycket på
logguppgifter

Eller

Har loggsystem helt felfri kod?



Polisen fick fel ip-adress oskyldig barnporrmisstänkt

Du är här: [SvD.se](#) > [Nyheter](#) > [Inrikes](#) > [Oskyldigt anklagad för barnporr](#)


Oskyldigt anklagad för barnporr Polisen: "Vi kan bara be om ursäkt"

Publicerad: 15 maj 2008, 16.14. Senast ändrad: 15 maj 2008, 18.54

Rikskriminalen hade fel ip-nummer – en av de anklagade i barnpornografitillslaget i tisdags blev felaktigt utpekad. "Vi kan bara be om ursäkt", säger Rikskriminalpolisen som anmält både sig själva, åklagaren och polisen i Värmland. Men hos polisen i Karlstad anser man att Rikskrim är ansvariga.

Textstorlek:   Skriv ut  Blogglänkar (15 st)

Det var i tisdags som polisen i 14 län gjorde tillslag mot ett antal adresser och grep ett trettiotal personer misstänkta för barnpornografibrott och i vissa fall även våldtäkt mot barn. Men ett av de ip-nummer som ledde till husrannsakan på en adress i Värmland var fel. Det var när mannen nekade som

 **Läs mer**

> 30 gripna i barnporr-
razzia

Polisen fick fel ip-adress

- På Rikskriminalpolisen är man mycket skamsen över misstaget men menar samtidigt att felet skulle kunna hända igen – och att det hänt förut.
- Stefan Kronqvist chef för Rikskriminalpolisens IT-brottssektion
 - ~~”det har mig veterligen hänt 6 gånger på 200 – 300 fall”~~
 - ~~2-3 % av uppgifter om IP-adress är felaktiga~~
 - Enligt de senaste uppgifterna från Stefan Kronqvist så rör det sig om 6 fall på ett par tusen
 - Så det kan röra sig om 1 på 1000 som är felaktiga

Ändringen i rött efter nya uppgifter från Stefan Kronqvist under sitt föredrag efter vårt

Teknisk undersökning

Utbildningshandbok Polishögskolan

- 7.1.5 Om Internet är involverat
 - ”När det gäller digitala bevis i Internet-miljö är det viktigt att ange vilken tidszon som avses, speciellt vid kontakt med kollegor, teleoperatörer och ISP:er”
- 7.3.3.3 Teknisk undersökning
 - ”kontrollera datorns datum och klocka (inklusive tidszon) och notera avvikelsen i förhållande till ”Fröken ur”. Detta får inte göras med beslagets disk(ar) inkopplade. Angående tidszoner se siten <http://www.onlineconversion.com/timezone.htm>”

Tid och datum är viktiga

- För att kunna samköra logghändelser från olika system eller nätverk kan man använda:
 - Tid, datum, IP-adress, protokoll, port, session, användar-ID mm.
- När tid används för att samköra olika register måste tiden korrigeras med:
 - Tidzon
 - Sommar/vintertid
 - Differens mot känd tidsreferens som t.ex. GPS eller Frökenur

Vem kontrollerar Operatörernas TID?

Ställer PTS krav?

- **God funktion och teknisk säkerhet**
 - Tele- och Internetoperatörer bör bedriva ett kontinuerligt och systematiskt säkerhetsarbete för att uppnå säkrare elektroniska kommunikationer.
- **Vad säger lagen?**
 - I [lagen om elektronisk kommunikation](#) (LEK) finns bestämmelser om god funktion och teknisk säkerhet som gäller för alla som tillhandahåller elektroniska kommunikationsnät eller -tjänster.
 - I 5 kap. 6a § LEK framgår följande:
Den som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster skall se till att verksamheten uppfyller rimliga krav på god funktion och teknisk säkerhet samt på uthållighet och tillgänglighet vid extraordinära händelser i fredstid. Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om på vilket sätt skyldigheten skall fullgöras och om undantag från skyldigheterna.
 - Syftet med bestämmelserna är att bidra till effektiva och säkra elektroniska kommunikationer samt att skapa en grundläggande säkerhetsnivå för dessa. Med säkerhet avses i detta sammanhang **främst uthållighet, tillgänglighet och driftsäkerhet.**

Om tid, IP-adress i DHCP, NAT eller post i kunddatabasen är felaktiga

- Kommer operatören att upptäcka detta?
- Har det betydelse för driften?
- Har det ekonomisk betydelse?
- Kommer kunden att upptäcka detta?
- Kommer polisen bry sig i ett fildelningsmål?
- Kommer Anti piratbyrån eller IFPI att bry sig?
- Finns det någon som kravställer ?
- Finns det någon som kontrollerar?
- Bryr sig någon?

Data retention

2005 – Elektronisk kommunikation i brottsutredningar (SOU 2005:38) – lagring av trafikdata

2007 – Lagring av trafikuppgifter för brottsbekämpning (SOU 2007:76)



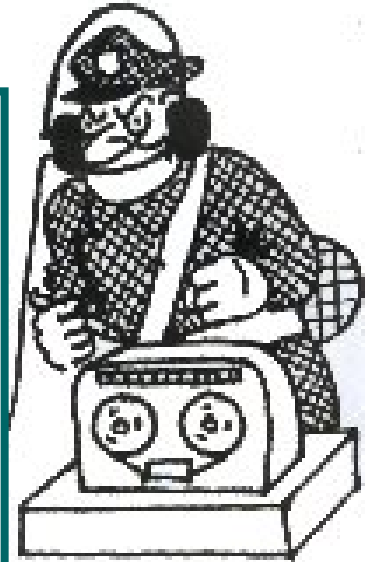
SKYLDIGHET ATT LAGRA TRAFIKDATA

= Omfattar annan information om meddelandet än dess innehåll (avsändare/mottagare, tid, varaktighet, plats etc.)

- Lagförslag på "g" (SOU 2005:38)
- Uppfyller svenska åtaganden enligt Cyber Crime Convention
- Avses träda ikraft under hösten 2007

Viss problematik

- Avsevärd mängd meddelanden!!!
 - TeliaSonera förmedlar ensamt ca 75 milj meddelanden - varje dag!!!
- Vem skall stå för kostnaderna????
 - Teleoperatörerna, d v s kunderna!!!
- Proportionalitet?
 - Rimligt att spara en oerhörd mängd data för några tusen ärenden?
 - Eftersom det är teleoperatörerna som står för fiolerna är det inga problem för myndigheterna – man kan slösa hur man vill...



Om säkerheten är bristfällig – hur användbar och tillförlitlig är då informationen???

IPRED

Ds 2007:29; Musik och film på Internet – hot eller möjlighet?

Syftar till att genomföra direktiv 2001/29/EG (IPRED)

1. Rättighetsinnehavaren (eller dennes organisation) får information om att fildelning skett från en viss IP-adress
2. Rättighetsinnehavaren dokumenterar fildelningen och IP-adressen
3. Rättighetsinnehavaren väcker talan vid domstol mot den misstänkte fildelarens operatör
4. Operatören ges tillfälle att yttra sig till domstolen
5. Om rättighetsinnehavarens bevisning anses tillräcklig föreläggs operatören att lämna ut information om vilken kund som innehar IP-adressen (den som tecknat abonnemanget)
6. Rättighetsinnehavaren får därefter vända sig till kunden och framställa krav mot denne, t.ex. genom att kräva att fildelningen upphör eller kräva ersättning för intrånget



I tvistemål är beviskravet lägre än i brottmål och risken ökar därmed för materiellt oriktiga domar!

Blind tro på IT-verktyg

Litar utredare för mycket på s.k. IT-forensiska verktyg

Encase (Hip Hip Hora)

- För att visa på betydelsen av att processen med bevissäkring dokumenteras kan vi se på följande exempel:
 - Om den i utredningen beslagtagna DVD-skivan analyseras i programmet "Encase" så ser det ut som om skivan har framställts innan tidpunkten som anges för nedladdning i anmälan
 - Vid verifiering med ett annat program "CD/DVD Diagnostic" så anges en annan tidpunkt
- Genom att läsa standaren och tolka den råa information kan jag konstatera att båda programmen ger fel tid
- Det finns en uppenbar risk att en utredare kan dra fel slutsats om när en skiva har skapats
- I detta fall såg det ut som om skivan var skapad innan det påstådda brottet

Ilook Investigator (Linköpingsfallet)

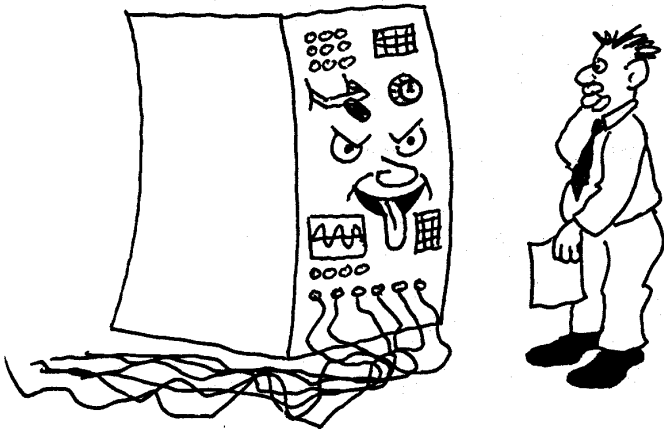
- Ilook Investigator användes i detta fall av polisen för analys av hårddiskar och dess innehåll
 - Ilook bryr sig inte om att en hårddisk är dynamisk och rapporterar inte detta till utredaren
- En hårddisk som är dynamisk måste importeras in i systemet innan den kan läsas
- Det är en uppenbar risk att en utredare kan dra en felaktiga slutsats om att en disk är tillgänglig för en användare
- I detta fall har åklagaren och SKL inte kunna styrka att hårddisken var åtkomlig för användaren

IT-forensik

POLIS

AVSPÄRRAT

POLIS



- Att en viss anslutning/visst abonnemang/visst konto använts
- Kompletterande bevisning nödvändig för att fastställa den faktiske användaren/gärningsmannen
- Hur tillförlitlig är den digitala bevisningen?
 - Har systemen säkerhetsbrister?
 - Kan den egentliga källan spåras?
 - Kan uppgifterna ha manipulerats?
- Erkännandet särskilt viktigt i dessa sammanhang!!!
- **Fippla inte med "brottsplatsen!!!!**
 - Du kan förstöra bevisvärdet!
 - Rådgör med expert innan du gör något själv
 - Bevissäkra HELA webb-platser
 - Tidsstämpla
 - Spegelkopiera
 - Bevissäkra omedelbart



Samma risk för att förstöra bevis som på en vanlig fysisk brottsplats!

Slutsatser

- IT är inte något unikt, detta var sant på 90-talet och detta är sant idag också
- Rättsväsendet måste ta hänsyn till att IT-system generellt har dålig säkerhet
- Politikers och rättsväsendets IT-kunskaper måste ökas
- I viss mån måste lagstiftning och rättstillämpning anpassas