

Checklista för digitalt källskydd

Sus Andersson – Sofia Bering
Journalistförbundets öppenhetsgrupp 2004

JOURNALIST
● ● ● ● ● ● ● ● ● ● ● ●
FÖRBUNDET ●

Bakgrund

Alla har en grundlagsfäst rätt att lämna uppgifter till media utan att bli straffade för det eller att riskera att få sin identitet avslöjad. Myndigheter får inte forska efter källor och de som arbetar i medieföretag får inte avslöja sina källor.

Källskyddet är en hörnpelare i svensk demokrati. Även om vi journalister till vardags strävar efter största möjliga öppenhet och källor som vågar tala öppet måste vi slå vakt om den säkerhetsventil som källskyddet utgör.

Idag lämnar vi allt fler elektroniska spår efter oss. Därmed löper källorna större risk att avslöjas. Deras arbetsgivare kan läsa e-postloggar och kolla vem var och en ringt till genom specificerade telefonräkningar. Genom datorvirus kan känslig information på journalistens dator spridas till vem som helst på internet.

Problemen kan uppstå både genom att källorna själva är obetänksamma – eller för att vi journalister är det.

Den här skriften är tänkt som en checklista för att minska riskerna för källorna. Den vänder sig till enskilda journalister såväl som till journalistklubbar, som kan behöva se över medieföretagens policydokument.

Om lagen

Tryckfrihetsförordningen slår fast allas rätt att lämna uppgifter till press, radio och teve utan att bli straffade för det eller att riskera att få sin identitet avslöjad (1 kap 1 § och 3 kap 3-5 §§).

Meddelarskydd och källskydd är i princip samma sak i det att det garanterar anonymitet för meddelaren eller uppgiftslämnaren. Men källskydd används kanske främst för att benämna journalisters skyldighet att inte röja sina källor medan meddelarskyddet tar sikte på förbudet för myndigheter att efterforska vem som lämnat uppgifterna.

Meddelarskyddet innebär alltså att anställda vid myndigheter kan lämna uppgifter, även hemliga (med några undantag, se nedan) – men inte hemliga *handlingar* – till media utan att riskera att deras identitet efterforskas. Det är nämligen brottsligt (TF 3 kap 4-5 §§) för myndigheter att forska efter vem som har lämnat uppgiften.

Meddelarskyddet gäller inte anställda i den privata sektorn i samma utsträckning. Deras meddelarfrihet får begränsas genom avtal. Privatanställda får både efterforskas och straffas för sina kontakter med media. De är genom den lojalitetsplikt, som anses ligga i varje anställningsförhållande, förhindrade att genom yttranden skada arbetsgivaren.

Journalisters skyldighet att inte avslöja sina källor omfattar däremot, naturligtvis, även privatanställda.

Meddelarskyddet är dock inte oinskränkt, inte ens för statligt anställda. Vissa sekretessbelagda uppgifter får helt enkelt aldrig lämnas ut. Det gäller till exempel

uppgifter som om de publiceras leder till att utgivaren eller upphovsmannen gör sig skyldig till landsförräderi eller spioneri eller liknande.

Journalistklubben kan se till att

- **ordna seminarier om källskydd** för att sprida kunskapen – gärna till hela medieföretaget och inte bara bland journalisterna,
- **företaget har policydokument** när det gäller allmänt källskydd och särskilt IT-skydd – se nedan.

I medieföretagets allmänna policydokument bör det framgå att

- **samtliga anställda på medieföretaget har skyldighet att värna källornas anonymitet.** Det gäller lika mycket teknikerna på dataavdelningen som den som granskar fakturor eller skriver artiklar,
- **alla avtal med externa leverantörer innehåller kraftiga sekretessklausuler.** Det kan gälla allt ifrån teleoperatörer till städpersonal, eftersom alla kan komma åt källors identitet i sina uppdrag.

I medieföretagets IT-policy bör det framgå att

- **dataavdelningens personal har ett särskilt ansvar** när det gäller skyddet av källor, eftersom de i allmänhet kommer åt mycket känslig information,
- **brandvägg och virussydd måste vara så kraftfulla** att grundlagens krav om anonymitet kan upprätthållas,
- **e-post inte bör användas** för att skicka material som omfattas av meddelarskydd,
- **känsliga elektroniska dokument förvaras på lösa minnesenheter** som CD, diskett eller minneskort och raderas från datorns hårddisk,
- **uttjänta datorers hårddiskar inte bara raderas, utan skrivs över med meningslös information.** Annars kan information som funnits lagrad tas fram med förhållandevis enkla medel.

Som journalist bör du

- **inte kontakta källor på deras arbetsplatser, om källorna ska vara anonyma.** E-postloggar kontrolleras regelbundet på många företag, och arbetsgivarna har långgående rätt att ifrågasätta och granska de anställdas användning av e-posten. På myndigheter är e-postloggen dessutom offentlig handling.

I den mån det är nödvändigt: använd hotmail eller motsvarande, och neutrala ämnesord och användarnamn. Kryptering kan vara en variant, men den är krånglig. För det första kräver den installation av program och ett utbyte av nycklar. Dessutom finns det risk att en arbetsgivare som plötsligt upptäcker att en medarbetare börjar kryptera sin post börjar misstänka att den personen sysslar med något som kräver granskning.

Den fasta telefonen skvallrar i de flesta fall inte om det är du som ringer och du kommer fram direkt. Men om telefonen är vidarekopplad till växeln eller en automatisk telefonsvarare kommer samtalet troligen att registreras på något sätt som går att komma åt för den som kan ha anledning att leta efter källor. En del datoriserade telefonsvarare lägger det inspelade som ett e-postmeddelande med telefonnumret i ärenderaden och en ljudfil i meddelandet.

En anonym källa bör inte uppmuntras att ringa tillbaka från sin arbetsplats, vare sig från sin fasta telefon eller mobiltelefon. Teleräkningarna skvallrar om vart telefonsamtalen har gått.

Än så länge är det svårt att få tillgång till information som visar var en mobilägare befinner sig. Men rent tekniskt är det möjligt att få fram geografisk position ur mobiloperatörernas trafikdata. Idag kan polisen låta ta fram sådan information i samband med brottsutredningar.

Hos en del mobiloperatörer finns redan idag specialtjänster som hela tiden positionerar telefoner, något som exempelvis används av åkerier. Om källan/källans arbetsgivare har denna tjänst inkopplad finns möjlighet att spåra exakt var telefonen befinner sig.

Sms-kontakter kan via telefonräkningar spåras, i alla fall tidpunkt för sändningen och till vilket nummer, dock inte innehållet i meddelandet. Däremot kan både sparade och slängda sms vaskas fram på teknisk väg ur telefonminnet, liksom kontaktuppgifter som finns i telefonen, om någon får tag på journalistens eller källans telefon.

- **inte e-posta dokument som innehåller känslig info** – inte till någon. Risken är stor att dokumentet hamnar på avvägar. "Betrakta e-post som vykort". Om du skickar material till en myndighet e-postledes bör det bli offentlig handling.
- **inte använda Microsofts kontaktbok** för att spara uppgifter om hemliga källor. Många virus använder just Microsofts kontaktbok för att sprida sig.
- **inte spara några känsliga dokument på en hårddisk som står i kontakt med Internet.** Det har hänt att virus som kommit in genom e-postprogram plockat ett godtyckligt dokument från datorns hårddisk och skickat det vidare. Risken att det är "fel" dokument är visserligen liten – men inte desto mindre katastrofal om det skulle spridas.
- **tänka på att det i många datorsystem framgår vem som varit inloggad** och vad de gjort. En källa kan avslöja sig då den tar fram information åt dig – genom sitt inloggnings-id, genom att systemet känner av vem som dragit sitt passerkort för att passera dörrar o dyl. Det kan också finnas övervakningskameror som registrerar var folk befinner sig.

Källor:

- Lennart Lillieroth: "Sekretess! Handbok om sekretesslagstiftning". 15 uppl. 2002.
- Trond Sefastsson: "Offentlighetsprincipen i praktiken" 2 uppl 1999
- Ny Teknik 2004:24 Många vill följa dina digitala spår.
- Martin Lindeblad, Journalistförbundet. Personlig kontakt.