

Checklista för digitalt källskydd

Sus Andersson och Sofia Bering
Journalistförbundets yttrandefrihetsgrupp

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

Första utgåvan 2004
Reviderad januari 2010

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.

Nya lagar och lagförslag som kan få konsekvenser för källskyddet lanseras nu i en allt snabbare takt.

Teknikutvecklingen innebär ständigt nya möjligheter att kartlägga och övervaka människor. Därför kommer vi inte att kunna uppdatera denna lathund i takt med varje ny lag som ser dagens ljus och inte heller ge detaljerad information om hur man ska gå till väga. Vi har istället utformat våra råd och tips om hur man bör hantera källor i den digitala tidsåldern ganska generellt för att visa hur man kan resonera och vad man bör vara vaksam på. På det sättet tror vi att råden blir mer användbara och kommer att tåla en del lagförändringar utan att genast bli föråldrade.

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

- **ordna seminarier om källskydd** för att sprida kunskapen - gärna till hela medieföretaget och inte bara bland journalisterna,
- **verka för att 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,
- **avtal ska skrivas med all icke-anställd redaktionell personal** för att reglera relationen mellan redaktionen och den utomstående medarbetaren. Förutom det journalistiska uppdraget bör även eventuella andra uppdrag regleras för att undvika att det uppstår konflikt mellan det journalistiska och eventuella andra uppdragen. I detta avtal ska även regleras hur utomstående medarbetare ska säkerställa källornas anonymitet när källskyddat material inte förvaras på redaktionen,
- **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

- **IT-avdelningens 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 måste du:

- **Skydda dina källor.** Du är enligt Tryckfrihetsförordningen och Yttrandefrihetsgrundlagen skyldig att inte röja anonyma källor.
Det innebär bland annat att du måste förvara de uppgifter som lämnas under anonymitetsskydd på ett säkert sätt. Arbetar du utanför redaktionens lokaler är detta särskilt viktigt. Du bör inte förvara källskyddat material i samma dator eller på samma ställe som annat, icke källskyddat material. Du måste räkna med risken att du får inbrott i din bostad. Arbetar du som frilans med källskyddat material, bör alltså detta antingen förvaras på uppdragsgivarens redaktion eller, om sådan saknas, på annat säkert ställe.

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 vissa fall kan det gå att använda hotmail, gmail eller motsvarande. Men tänk på att inte heller dessa är helt anonyma. Om någon försöker spåra avsändaren är det inte svårt att få fram om e-brevet skickats från en dator på en viss arbetsplats. 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 från sin mobiltelefon. Teleräkningarna skvallrar om vart telefonsamtalen har gått.

Mobiltelefoner lämnar spår efter sig. Inte heller kontantkortstelefoner är helt säkra. Det går att spåra mobiler via telefonens id-nummer (Imie-numret).

Det finns program som visar var en mobiltelefon befinner sig. En del företag använder dem som säkerhet och/eller för kontroll av sina anställda. Som journalist bör du vara vaksam så att ingen installerar ett sådant program i din telefon. Programmen kan installeras på några sekunder.

Sms-kontakter kan spåras via telefonräkningar, 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.

Det är också värt att varna för de spionprogram för installation på mobiltelefoner som finns på marknaden. Den som under en kort stund har tillgång till din mobil kan ladda ner en programvara som registrerar alla samtalslistor och sms och sända dessa, utan att du märker något, till den som spionerar. Det finns också program som via en tyst uppringning aktiverar mikrofonen i din telefon (än så länge bara när telefonen är påslagen) den som ringer upp kan alltså tjuvlyssna på det som sägs i rummet där du (och mobilen) befinner er. Bäst att hålla reda på sin mobiltelefon alltså och kanske stänga av den vid känsliga möten.

- **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.

- **Kryptera** känsliga dokument.
- **tänka på att inte spara känslig information på bärbara datorer och smarta telefoner** som du bär med dig överallt. Risken är stor att de stjäls - eller bara glöms bort.
- **tänka på att det i många datorsystem framgår vilka som varit inloggade** 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.

Mer information om källskydd i praktiken och hur du exempelvis krypterar dokument finns på Journalistförbundets webbplats, www.sjf.se. Sök på "digitalt källskydd". Där finns också denna broschyr som pdf.

Källor:

- Yttrandefrihet & tryckfrihet. Handbok för journalister, Anders R Olsson
- Sekretess! Handbok om sekretesslagstiftning, Lennart Lillieroth
- Offentlighetsprincipen i praktiken, Trond Sefastsson
- Beslag av en dator hos en person med anknytning till ett medieföretag, Justitiekanslerns beslut 2007-12-19
- PM angående YGL:s regler om tystnadsplikt. Hans-Gunnar Axberger 2006-02-15
- Martin Lindeblad, Journalistförbundet. Personlig kontakt.
- Pär Ström, IT-konsult. Personlig kontakt.

Snabbversionen: Mumla!

Fem tips för dig som snabbt vill bli bättre på att skydda dina källor - och fem tips som du kan ge dina källor. Det egentligen ganska enkelt: kom ihåg att mumla när du behöver vara litet diskret!

Mumla för journalister

Mobil med kontantkort

Undvik e-post, annars

Maskerad e-post, anonyma konton på gmail, hotmail och liknande

Lagra krypterat

Anonymt surfande

Mumla för källor

Mobil med kontantkort

Undvik e-post, annars

Maskerad e-post, anonyma konton på gmail, hotmail och liknande

Lagra krypterat

Aldrig arbetsgivarens telefon eller dator för mediekontakter