

# BIG DATA

– så kartläggs våra liv



En idéskrift  
om massövervakning  
och personlig integritet



De Gröna | Europeiska fria alliansen  
i Europaparlamentet

miljöpartiet de gröna



# FÖRORD

**2016**

**A**LDRIG FÖRR HAR det varit så enkelt att övervaka människor som det är i dag. Teknikutvecklingen har gjort det lätt och billigt att samla information om våra vanor, vänner, åsikter, hälsotillstånd och privatliv.

De senaste 15 åren har det stiftats en mängd nya lagar världen över som möjliggjort en ständigt ökande övervakning. Lagarna har ofta motiverats med hänvisning till säkerhet och hotet från terrorism, men i praktiken används det i allt större utsträckning för mindre brott såsom att jaga enskilda fildelare.

Integritetshotande förslag kan verka fullt rimliga om man ser på dem var för sig, men när de travas på hög leder de till ett samhälle där män-

niskor utsätts för en orimlig grad av övervakning. Frågan är om vi vill att människor ska vara övervakade nästan överallt? Hur påverkar det demokratin när människor vet att stat och företag kan läsa nästan allt de skriver?

Vi vet att information kan missbrukas, och att risken är stor att den läcker ut och hamnar i orätta händer. Vissa IT-företag vet redan mer om oss än vi har berättat ens för våra närmaste vänner, och det är kunskaper som de använder för att sälja reklam.

Det finns ingen naturlag som säger att företag och myndigheter ska få massövervaka människor bara för att det finns tekniska möjligheter att göra det. Det handlar om ett

” **Det finns ingen naturlag som säger att företag och myndigheter ska få massövervaka människor bara för att det finns tekniska möjligheter att göra det.**

politiskt val. Det finns en växande opinion av aktivister, konsumenter, IT-kunniga, journalister, jurister och andra medborgare som vill sätta rimliga gränser och kräver att människors rätt till integritet och privatliv respekteras.

Det här är den andra idéskriften i en serie om EU och grön politik – övriga delar handlar om alltifrån klimatpolitik till handelsfrågor och EU-kritik. Jag hoppas att de här skrifterna ska bidra till att lyfta debatten i några av vår tids viktigaste politiska frågor.

**Max Andersson,**  
EU-parlamentariker



# INLEDNING

---

**I**NFORMATIONSTEKNOLOGI SPELAR EN allt viktigare roll i våra liv och samhällen. Aldrig tidigare har så många haft möjlighet att så lätt kommunicera med varandra. Spridandet av information har bidragit till snabba tekniska och ekonomiska framsteg och öppnat nya möjligheter för delaktighet och demokrati. Men samtidigt innebär detta nya risker vad gäller vår personliga integritet. I dag går det att kartlägga våra liv via mobilen, aktivitetsarmbandet, tvättstugebokningen, internetbanken, gymkortet och passerkortet på jobbet för att nämna några sätt.

I juni 2013 fylldes världsmedia av Edward Snowdens avslöjanden om USA:s underrättelsetjänst NSA. Bilden som tonade fram var en enorm

övervakningsapparat där allt kunde avlyssnas, registreras och kartläggas. Det handlar inte bara om USA. En rad integritetskränkande lagar har drivits igenom både i Sverige och i EU sedan slutet av 1990-talet, däribland datalagringsdirektivet, FRA-lagen och IPRED-lagen. Rädslan för terrorism och grov brottslighet samt industrins kamp mot piratkopiering har drivit på denna utveckling.

I dag samlar myndigheter och företag allt mer information om var vi befinner oss, hur vi konsumerar eller vilka sidor vi surfar på. Somliga anser att oron för detta är överdriven. Men vad får det här för konsekvenser för våra öppna samhällen och vad kan det leda till på längre sikt?

# PERSONLIG INTEGRITET PÅ NÄTET

---

VARE SIG VI är medvetna om det eller inte skapas stora informationsmängder om oss varje dag i samband med att vi utför olika vardagsaktiviteter. Som när vi handlar i en affär (registreras genom konto- och kundkort), åker med kommunala färdmedel (registreras i elektroniska biljettsystem), söker information på webben (registreras via sökmotorn), läser tidningen på datorn (registreras i annonser och sociala medier), umgås med vänner via sociala medier (registreras av många), eller bara tar en promenad med mobiltelefonen i fickan (registreras av teleoperatören och mobiltillverkaren).

Det kan finnas ett stort värde i all denna informationsmängd. "Big Data" har kommit att bli ett begrepp som omfattar alla de möjligheter som stora informationsmängder kan erbjuda i framtiden. Samtidigt leder detta till stora utmaningar för våra etablerade sätt att hantera vår personliga integritet, som vi inte är vana vid från den fysiska världen.

För ur denna omfattande informationsmängd går det att utläsa en rad olika detaljer om våra vanor och beteenden, åsikter, sociala nätverk, rörelsemönster, hälsotillstånd och ekonomi. Sätten att samla in upp-



gifter varierar, liksom vilka aktörer som står för insamling, lagring och användning av informationen. Den enda realistiska inställningen är att allt vi gör på nätet kan och kommer att lagras.

Att personlig integritet är en mänsklig rättighet slås fast i flera internationella konventioner, såsom Europakonventionen om skydd för de mänskliga rättigheterna. Personlig integritet handlar inte bara om rätten att få vara ifred. Det är ett

viktigt perspektiv, men det handlar också om möjligheten, eller rentav rätten, att kontrollera spridning och användning av ens egen personliga information. Det kan handla om att ha rätt att hysa vissa åsikter och ha vissa attityder utan att behöva oroa sig för repressalier eller påverkan från andra.

I världen utanför internet är vi vana vid att kunna välja att dela viss information med olika personer. Vi tar för givet att vissa saker är

## ” Den moderna tekniken har skapat möjligheter för företag och stater att kränka människors privatliv i en aldrig tidigare skådad omfattning.

privata och på sin höjd delas med familj och vänner medan annat är offentligt. I den bemärkelsen handlar den personliga integriteten också om handlingsfrihet där man från en situation till en annan kan variera sin delaktighet och synlighet. Vi vill alla bli bedömda utifrån den information som är relevant för en given situation. Sjukdomshistoria, sociala relationer och politiska åsikter är exempel på personlig information som vi av goda skäl ibland kan vilja hålla för oss själva. För en ung hbtq-

person kan det vara extra viktigt att få vara anonym på nätet och själv välja när den vill komma ut och med vem den vill att denna information ska delas.

På kommande sidor ska vi läsa mer om hur stater, myndigheter och företag drivit på utvecklingen att samla in och kartlägga personuppgifter för egna syften och vilka risker det kan föra med sig samt vad vi vill göra åt det.

# DATALAGRINGSDIREKTIVET

---

**E**U:S DATALAGRINGSDIREKTIV TRÄDDE i kraft 2006 och innebar att tele- och dataoperatörer måste spara uppgifter om vem som kommunicerar med vem via telefon och internet i minst sex månader. Själva innehållet i telefonsamtal, sms och e-post sparas inte, men uppgifterna om var personen befann sig när kommunikationen inleddes och avslutade ska lagras, för att kunna avslöja allvarliga brott. Dessa uppgifter, så kallade metadata, innebär möjlighet till kartläggning av personliga nätverk, geografisk position eller kontakter med myndigheter för personer även om dessa inte misstänks för något brott.

Förslaget kom upp på den politiska agendan efter bombattentaten i Madrid 2004 och London 2005, efter ett stort tryck på politiker att vidta åtgärder. Syftet var till en början att bekämpa terrorism men i praktiken har uppgifterna använts även vid utredning av mindre allvarliga brott.

Direktivet har under åren fått utstå mycket kritik från såväl politiker, medborgare som tele- och internetoperatörer för att bryta mot mänskliga rättigheter och äventyra den personliga integriteten. I april 2014 förklarade också EU-domstolen datalagringsdirektivet ogiltigt. EU-domstolen menar att direktivet inte är förenligt med grundläggande fri- och rättigheter och är ett allvarligt intrång i privatlivet.

Under sommaren 2014 meddelade den svenska regeringen att den ansåg att reglerna om datalagring som har införts i Sverige inte har samma svagheter som EU-direktivet och att de fortfarande gäller. Detta är en ståndpunkt som starkt kritiserats. I april 2015 begärde därför kammarrätten i Stockholm ett så kallat förhandsavgörande från EU-domstolen. EU-domstolen ska därmed bedöma om det svenska kravet på att fortsätta lagra datauppgifter strider mot EU-rätten.



” Sakerna jag såg började verkligen störa mig. Jag kunde följa drönare i realtid när de övervakade människor som de skulle döda. Man kunde se hela byar och se vad människor gjorde. Jag såg NSA följa människors aktiviteter på internet medan de skrev. Jag blev medveten om hur inkräktande USA:s massövervakningsprogram hade blivit.



EDWARD SNOWDEN

EDWARD SNOWDEN ÄR en amerikansk visselblåsare som tidigare arbetade åt USA:s underrättelsetjänst National Security Agency (NSA). Efter att i flera år fått allt större insyn i och förfasats över hur USA byggt upp storskaliga och topphemliga övervakningssystem med förmågan att registrera telefon- och dataanvändning i hela världen valde Snowden att läcka sina upptäckter till allmänheten. Tillsammans med journalisten Glenn

Greenwald och dokumentärfilmaren Laura Poitras överlämnade Snowden i juni 2013 tusentals hemligstämplade dokument som visade omfattningen av USA:s massövervakningen till tidningarna The Guardian och Washington Post. År 2014 tilldelades Snowden det alternativa Nobelpriset Right Livelihood Award, men kunde aldrig hämta ut priset på grund av risken för att bli utlämnad till USA och dömas till fängelse för spioneri.



En av de viktigaste uppgifterna som Snowden läckte var informationen om Prism, ett signalspaningsprogram som används av amerikansk underrättelsetjänst. Programmet har gett NSA och FBI tillgång till realtidskommunikation såväl som lagrad information via företag som Microsoft, Facebook, Apple och Google. Data som amerikanska myndigheter kan inhämta med Prism inkluderar bland annat inloggningsuppgifter, e-post, kommunikation på sociala medier, fotografier, videoklipp samt video- och röstchattar. Det har gett dem möjlighet att kartlägga, följa och registrera inte bara sina egna medborgare utan även medborgare i hela världen. Eller som Snowden själv uttrycker det i en intervju med journalisten Glenn Greenwald: "Sakerna jag såg började verkligen störa mig. Jag kunde följa drönare i realtid

när de övervakade människor som de skulle döda. Man kunde se hela byar och se vad människor gjorde. Jag såg NSA följa människors aktiviteter på internet medan de skrev. Jag blev medveten om hur inkräktande USA:s massövervakningsprogram hade blivit."

Sedan Snowden läckte de sekretessbelagda dokumenten har han jagats av amerikanska myndigheter och han befinner sig nu i exil i Ryssland. EU-parlamentet antog under 2015 en resolution som uppmanar medlemsstaterna att lägga ner eventuella straffrättsliga åtal mot Snowden och bevilja honom skydd, med hänsyn till hans ställning som visselblåsare och internationell försvarare av de mänskliga rättigheterna. Än så länge har inget land velat ge honom asyl, med risk för att stöta sig med USA.

# FLYGDATA LAGRING

## – PNR

---

**E**U-KOMMISSIONEN FÖRESLOG 2011 att flygbolag ska bli skyldiga att lämna ut uppgifter om sina passagerare till EU:s medlemsländer. Informationen ska kunna användas för att upptäcka och utreda brott som till exempel terrorism, narkotikasmuggling och människohandel. Förslaget förväntas träda i kraft 2018 men har fått hård kritik.

PNR, som systemet kallas står för Passenger Name Records och innehåller information om passagerarna som insamlas av flygbolag. Det finns redan i dag information som inkluderar namn, nationalitet och passnummer som samlas in och används av polis för att söka efter exempelvis efterlysta brottslingar. PNR innehåller en vidare kategori information, som inkluderar data med känslig information där en individs religion, sociala status och sexuella läggning kan avslöjas.

PNR-data jämförs med profiler i förbestämda bedömningskriterier för att upptäcka misstänksamma mönster eller beteenden. Detta är ett mycket godtyckligt verktyg. I praktiken är det troligt att vanliga medborgare kommer att stoppas på flygplatser på grund av sitt namn, ursprung, religion eller sociala bakgrund. Uppgifterna, som kan sparas upp till fem år, skickas från flygbolagen till ansvariga myndigheter i EU:s medlemsländer.

På samma sätt som datalagringen bygger PNR på övervakning av människor som inte är misstänkta för något brott. Mycket kritik har därför riktats mot PNR, från bland annat Europeiska datatillsynsmannen och EU:s byrå för grundläggande rättigheter. Mycket av farhågorna handlar om att det är problematiskt när personuppgifter lagras, bearbetas och sprids i EU:s 28 medlemsländer.

# SIGNALSPANING

## – FRA-lagen

---

**F**RA-LAGEN INFÖRDES VÅREN 2008 och ger Försvarets radioanstalt (FRA) rätt att avlyssna all datakommunikation som passerar landets gränser. Syftet med lagen är att reglera på vilket sätt FRA får ta del av kommunikation i kabel som passerar Sveriges gränser, det vill säga telefon- och internettrafik. Då både internet och telefonsamtal mellan två punkter i Sverige oftast tar omvägen via utlandet innebär det att i stort sett all telefoni och internetanvändning i dag kan vara övervakad.

Till en början sades det att FRA bara skulle få spana efter hot mot landets säkerhet och internationell terrorism.

Sedan dess har även polisen och säkerhetspolisen getts rätt att lägga beställningar hos FRA. Från början fick bara myndigheterna plocka ut uppgifter när det handlade om brott som straffades med fängelse. I dag går det att plocka ut trafikdata i utredningar även vid lindrigare brott. Bahnhofs VD Jon Karlung sa i en intervju med Ny Teknik i december 2013 att ”vi kan få mejl av polisen med begäran om utlämning där det inte ens finns med någon laglig grund”. Under 2013 visade de dokument som Edward Snowden lämnat ut att FRA även förser den amerikanska underrättelsetjänsten med stora mängder material.



# FÖRETAGEN SOM SPÅRAR DIG PÅ NÄTET

---

DET ÄR INTE bara NSA, FBI och andra myndigheter som spårar dig på internet. Det pågår också en parallell utveckling där allt fler företag spårar och samlar data, med eller utan vår tillåtelse. I princip allt du läser, skriver och söker efter på nätet kan sparas och spåras via exempelvis cookies och applikationer.

Möjligheten till insamling av mer riktad personlig information gör internet och sociala medier till guldgruvor för alla som vill bilda sig en uppfattning om individers intressen, vanor och umgängen. Denna kunskap utnyttjas alltmer för att sälja riktad reklam och beteendedata till olika aktörer. Sådana personuppgifter har de senaste åren blivit en mångmiljardindustri. Många stora

företag som Facebook och Google sparar data om våra internetvanor och paketerar det för att sälja vidare. Du är inte kund hos Facebook, utan deras produkt. Personuppgifter har varit en viktig del av internets ekonomi i många år, särskilt för gratis-tjänster. Men spårningsföretagen finns också på många webbplatser som tillhör kommuner, myndigheter och landsting.

Ofta sker det med vårt godkännande genom grundinställningar i vår dator som accepterar cookies eller att vi godkänner avtal och sekretessvillkor för nya applikationer eller sidor vi surfar på. Avtalen är ofta så långa och komplexa att man måste vara jurist för att förstå dem, och det är sannolikt ett mycket litet antal

## ” Du är inte kund hos Facebook, utan deras produkt.

användare som faktiskt gör ett välgrundat val när de accepterar dessa villkor.

I slutet av 2015 kom EU-kommissionen, EU-parlamentet och ministerrådet överens om en ny förordning om dataskydd. Den nya förordning-

en beräknas träda i kraft under 2018 och förväntas ställa hårdare krav på alla som hanterar någon form av persondata. Bland annat ställs strängare krav på att företag och andra organisationer ska informera om hur de hanterar enskildas personuppgifter.

**S**APE HARBOR ÄR ett beslut taget av EU-kommissionen år 2000 som tillåter överföring av personuppgifter från EU till USA. Safe Harbor avtalet innehåller de regler om personlig integritet och dataskydd som styr när företag för över kunduppgifter från EU till USA – något som många företag gör på regelbunden basis. I regel samlas uppgifterna in i Europa och skickas över Atlanten för att analyseras så att de kan användas i exempelvis riktad reklam. Det är inte bara IT-företag som använder sig av avtalet - även reseindustrin, logistikföretag, och många andra företag med en global närvaro påverkas på ett eller annat sätt av dessa regler.

Regelsamlingen godkändes år 2000, men har hamnat i blåsväder efter Edward Snowdens avslöjanden om

NSA:s massövervakning. Ärendet som drog det hela till sin spets är ett rättsfall där en österrikisk juridikstudent stämde Facebook för att de fört över hans uppgifter till amerikanska servrar, och därmed gjort dem tillgängliga för den amerikanska underrättelsetjänsten.

Under 2015 beslutade EU-domstolen att USA inte kan ge tillräckligt skydd för den personliga integriteten och upphävde Safe Harbor-beslutet. Det är en av de första juridiska konsekvenserna av Edward Snowdens avslöjanden om massövervakning. EU-kommissionen försöker nu ersätta Safe Harbor med ett nytt beslut kallat Privacy Shield, men kritiker hävdar att inte heller det garanterar medborgarnas rättigheter.

OM SAFE HARBOR

# VANLIGA ARGUMENT FÖR MASSÖVERVAKNING

---

**Vad händer i en framtid där allt mer personlig information samlas på hög och lätt kan missbrukas? Frågan gäller givetvis för all information som lagras oavsett om det är av staten eller andra aktörer och det sträcker sig från sjukjournaler till konsumtionsmönster hos Ica. Här nedan går vi igenom de vanligaste argumenten för den ökande övervakningen och motargument mot dessa.**

## Massövervakning behövs för att bekämpa terrorism

Det finns inga skäl att tro att massinsamling av personuppgifter är effektivt för att bekämpa terrorism. Den som inte vill bli sedd kan lätt kringgå PNR-systemet genom att ta bilen, sova hos en kompis eller betala kontant. FRA kan kringgå genom att man krypterar sin trafik eller gör

så att det ser ut som att trafiken är inhemsk. Datainsamlingen kommer därför i huvudsak att handla om att övervaka allmänheten som helhet och att söka efter eventuella gärningsmän efter att brott begåtts, inte förebyggande brottsbekämpning. Det problematiska med massövervakning är också att det kan skapa en falsk känsla av trygghet, när det egentligen är andra insatser som behövs för att förebygga och stoppa terrorism.



I januari 2014 visade en analys av 225 fall av terrorism i USA sedan den 11 september 2001 att den omfattande massövervakningen av all telefontrafik som genomförts av NSA inte har haft någon märkbar effekt för att förhindra terrorhandlingar. Det som har lett till att terroristhandlingar har kunnat avslöjas vid ett antal tillfällen i USA har istället varit traditionellt polisarbete. Faktum är att den globala amerikanska massövervakningen ännu inte lett till att en enda terrorist fällts i domstol. Inte heller i Sverige finns det några bevis för att massövervakningen är ett effektivt sätt att stoppa terrorister. Signalspaningen via FRA kostar oss närmare en miljard kronor årligen. Frågan är om de pengarna kan användas mer effektivt?

EU har infört över 200 åtgärder mot terrorism sedan terroristattacken den 11 september 2001. Men det har ännu

inte utvärderats om dessa åtgärder varit effektiva. Register för massövervakning är ofta både dyra och ineffektiva och kan liknas vid att leta efter en nål i en höstack. Det finns goda skäl att tro att pengar som spenderas på massövervakningen sannolikt skulle generera större effekt om de användes till vanligt polisiärt arbete och förebyggande arbete för att undvika brott.

## Varför ska jag bry mig om massövervakning? Jag har rent mjöl i påsen

Varför bry sig, den som inte har något att dölja har ju inget att vara orolig för? Inget argument för massövervakningens harmlöshet upprepas så ofta som just detta. Vi bryr oss inte om vanliga medborgares mejl och telefonsamtal,

**” Att säga att du inte bryr dig om rätten till integritet för att du inte har något att dölja är som att säga att du inte bryr dig om yttrandefriheten för att du inte har något att säga.**

försäkrade president Obama när han skulle försvara NSA:s enorma övervakningsapparat. Samma sak har bedyrats av ministrar, generaler och myndighetschefer. Men den samlade erfarenheten från 1900-talets övervakningssystem visar att det förhåller sig tvärtom, att övervakningssystemen gång på gång har gått ut över vanliga medborgare.

I mitten av 1970-talet avslöjades FBI:s spionprogram där man hade listat en halv miljon amerikanska medborgare enbart baserat på deras politiska övertygelse. FBI:s lista över mål varierade från Martin Luther King och John Lennon till freds- och kvinnorrättskämpar.

Detta var inget unikt i amerikansk historia och i många fall är motivet detsamma: oro och misstänksamhet mot oliktankande. Under Kalla kriget hade Säpo stora register över svenska medborgare som var engagerade på vänsterkanten, bland dem många journalister. Även Skånepolisen ertappades under 2013 för sitt register över romer i Sverige. Polisens register var olagligt och det fälldes senare i Europadomstolen.

Att säga att du inte bryr dig om rätten till integritet för att du inte har något att dölja är som att säga att du inte bryr dig om yttrandefriheten för att du inte har något att säga. Man kan

tro att den som har rent mjöl i påsen inte har något att frukta, men att det finns så stora mängder uppgifter om dig utgör alltid en risk. I den bästa av världar så hanteras det på rätt sätt, det kommer inte i orätta händer och det används bara till de mest vällovliga syften. Men personuppgifter kan komma i orätta händer, det kan vara rent slarv, dataintrång, tekniska misstag eller politiska beslut. En rad svenska myndigheter och kommuner har de senaste åren ertappats med läckta personuppgifter. Bland annat råkade Skatteverket ut för en omfattande hackerattack 2012 där information om omkring 1000 personer i Sverige som lever med skyddad identitet läckte ut.

Det finns även många beteenden som inte är olagliga men som kan ses som omoraliska såsom otrohet. Vill vi verkligen att dessa beteenden ska kunna registreras och spåras? Information om vår hälsa sparas och övervakas genom de sökningar vi gör, vad vi köper på nätet och genom internettjänster i vården. Inte ens den som anser sig ha rent mjöl i påsen vill nog att ens sjukdomshistoria ska bli allmänt tillgänglig för ens arbetsgivare eller försäkringsbolag. Som vi beskrivit tidigare handlar personlig integritet inte enbart om rätten att få vara ifred eller möjligheten att kontrollera informationsflöden. Det handlar lika mycket om att i olika situationer själv få välja vad som är privat respektive publikt.

# UPPHOVS RÄTT PÅ NÄTET

---

**D**EN TEKNISKA UTVECKLINGEN via internet har gett helt nya möjligheter för att sprida musik, film eller text. Det bidrar till ett kulturellt rikare samhälle och ger artister, författare eller andra kulturskapare möjligheter att synas. Fler får också möjlighet att ta del av kulturen. Men dagens upphovsrätt har inte hängtt med i utvecklingen. I dag driver upphovsrättsindustrin aktivt på för att kunna göra intrång i vårt dataanvändande, eftersom de tror att det är enda sättet att bevara upphovsrätten som den ser ut i dag. Ett flertal lagar som införts för att stärka upphovsrätten har också inneburit ett massövervakande av alla internetanvändare för att kunna upptäcka potentiella fildelare.

Miljöpartiet anser att det ska vara lagligt att ladda ner upphovsrätts-

skyddat material för privat bruk. Däremot ska det vara olagligt att sprida ett material i kommersiella syften utan lov från upphovspersonen. Det är viktigt att kulturarbetare ska kunna försörja sig men det måste skötas på ett sätt så att inte alla datorer massövervakas, exempelvis genom lagliga alternativ som Spotify och Netflix.

Med en balanserad upphovsrätt kan vi värna både kulturskapares rättigheter och rätten att kopiera utan massövervakning. I dag ser vi tvärtom att jakten på fildelare och piratkopiering har bidragit till ökad övervakning och spårning av all internettrafik. Integritetskränkande lagar och regler som skulle vara helt otänkbara i den fysiska världen är i dag en realitet på internet.



# IPRED-LAGEN

---

F<sup>L</sup>ERA LAGAR HAR stiftats för att stärka jakten på fildelning och kopiering av upphovsrättsskyddade verk. Den mest kända i Sverige baseras på EU-direktivet ”Intellectual Property Rights Enforcement Directive” och kallas IPRED-lagen. Lagen som trädde i kraft i juni 2009 möjliggör för rättighetsinnehavare att från internetleverantörer kräva ut personutgifter om människor som misstänks ladda ned upphovsrättsskyddade verk. Hur stor effekt IPRED-lagen haft på fildelning är omtvistat. De studier som gjorts pekar på en nedgång i fildelning precis efter att lagen infördes men att effekten på lite längre sikt


är liten. Det är troligt att lagliga sajter som Spotify och Netflix haft större inverkan på våra internetvanor.


De första åren användes lagen i begränsad utsträckning och straffen var ofta låga dagsböter. Men de senaste åren har vi sett en uppgång i antalet fall där svensk filmindustri åtalat flera svenska fildelare och begärt dem på mångmiljonbelopp. Exempelvis dömdes en man i Uppsala tingsrätt för inblandning i spridningen av en enda film ”The Stig-Helmer Story” till fem månaders fängelse för brott mot upphovsrätten med ett skadeståndskrav på 12,5 miljoner kronor.





## ATT SKICKA POST VS. ATT SKICKA E-POST




 När du skriver ett brev till någon är det du som väljer om du ska identifiera dig i brevet, inuti kuvertet, utanpå kuvertet, både och eller ingetdera. Det är helt och hållet ditt beslut att välja om du vill kommunicera anonymt eller inte. Det här är en rättighet som vi har i analog kommunikation enligt lagen.

 När du skriver ett brev till någon är det ingen som har rätt att plocka upp brevet under transporten, bryta förslutningen och undersöka innehållet, såvida det inte finns en formell konkret misstanke om brott. I så fall kan de brottsbekämpande myndigheterna göra det, men bara då, och bara just myndigheterna själva.

 När du skriver ett brev till någon har ingen tredje part rätt att ändra innehållet i brevet under transporten eller förhindra dess leverans.

 När du skriver ett brev till någon är det ingen som har rätt att stå vid brevlådan och kräva att all din kommunikation registreras, vem du kommunicerar med, när och hur länge.

 När du skriver brev till någon är brevbäraren som bär brevet till mottagaren aldrig ansvarig för vad du skrivit. Han har budbärarimmunitet.

Vi tycker det är rimligt att allt detta också ska gälla på internet. Allt ovanstående har sin grund i det faktum att alla digitala kommunikationskanaler som kan användas för privat korrespondens också kan användas för att överföra upphovsrättsskyddade verk i digital form – och det går inte att avgöra vad som är vad utan att ge upphovsrättsbranschen befogenhet att bryta förseglingarna till all privat kommunikation.

# DET ÖPPNA SAMHÄLLET MÅSTE FÖRSVARAS

---

DE SENASTE 40 åren har vi sett en mycket omfattande ökning av både privat och offentlig datainsamling. Allt fler människor uttrycker sina innersta tankar i mejl, blottar sin medicinska och ekonomiska status på internet, chattar konstant på sina mobiler, använder aktivitetsband och elektroniska kort- och biljettsystem. Det har öppnat upp för system för övervakning och lagring av personlig data, oavsett om det är regeringar och myndigheter som övervakar sina medborgare, IT-jättar som samlar data i kommersiella syften eller för att spåra fildelare.


Övervakningen på nätet ter sig särskilt stor i jämförelse med motsvarande övervakning i det fysiska rummet. Jämförelsen är relevant, eftersom vi idag gör ungefär samma saker i den fysiska världen som vi gör på internet. Om vi skulle översätta situationen på internet till det fysiska rummet, så skulle vi hela tiden följas av ett antal sensorer som registrerar vad vi gör, vad vi tittar på, vad vi köper, vem vi talar med och vart vi färdas. Vi skulle

inte veta vilka intressen dessa sensorer representerade eller hur den insamlade informationen skulle användas. Än mindre skulle vi ha möjlighet att få reda på vilka andra aktörer som informationen skulle kunna skickas vidare till.

Vi ser också en framtid där allt fler vardagliga fysiska objekt såsom hushållsapparater, fordon och kläder är anslutna till internet och kan uppfatta sin omvärld, kommunicera och medverka till att skapa smarta och hjälpsamma miljöer, varor och tjänster. Detta går under samlingsbegreppet ”internet of things”. Detta ställer allt högre krav på hantering av data via internet och vad vi gör med den.

På många sätt är likheten mellan övervakningssamhället i George Orwells dystopi 1984 och dagens samhälle slående. Skillnaden är att övervakningen idag inte utförs av en totalitär stat, men verktygen är på många sätt mycket mer långtgående än vad George Orwell troligen hade kunnat föreställa sig.





” På många sätt är likheten mellan övervaknings-samhället i George Orwells dystopi 1984 och dagens samhälle slående.

Tror du att samhället blir bättre av att staten vet allt om medborgarna, och att källskyddet, rätten att vara anonym och möjligheten att kommunicera privat begränsas? De flesta har kanske faktiskt ingen särskild anledning att oroa sig för att övervakningen ska hota dem personligen. Men vi har alla väldigt stor anledning att oroa oss för hur den hotar oss alla tillsammans, och underminerar skyddet för det öppna samhället. Integritetshotande förslag kan verka fullt rimliga var för sig, men när de travas på hög utgör de tillsammans ett betydligt större hot mot den personliga integriteten.

Vi har mycket begränsade möjligheter att stå utanför internet eller att kunna säga nej till den spårning som förekommer där. Det är uppenbart att vi behöver stärkta lagar för att skydda

den personliga integriteten på nätet på samma sätt som personuppgiftslagen, datalagen och offentlighetsprincipen på 1900-talet. Detta skulle kunna leda till en ökad öppenhet om vad som lagras och för vilka syften, vilket skulle kunna skapa ett bättre underlag för debatt om övervakningen på nätet.

Det är viktigt att betona att valen inte är inbyggda i tekniken på förhand, det är människor som avgör vilka värden datan ska främja eller hindra. Den kan möjliggöra friheter eller begränsa dem. Den kan främja personlig integritet eller övervakning. Det är människor som skriver koden, bygger internet och regleringen av den. Det är människor kollektivt och inte en liten elit, som kan och ska bestämma vilken värld vi ska leva i.

Istället för att skapa ett övervakningssamhälle behöver vi stärka skyddet för mänskliga rättigheter. Oavsett var, när eller hur vi kommunicerar. Vi arbetar för att utveckla skyddet för personlig integritet inom såväl Sverige som EU.

- ➔ Att vår kommunikation ska ha samma skydd, oavsett om den är i digital eller fysisk form. Det är rimligt att ha samma rätt att slippa få sitt brev läst av polis och säkerhetstjänst när man skickar det med mail som när man stoppar det på brevlådan. Samma regler för avlyssning ska gälla oavsett om man pratar via Skype eller en vanlig telefon.
- ➔ Att övervakning inte ska rikta sig mot människor som inte är misstänkta för något brott.
- ➔ Att myndigheter och företag måste vara öppna med vilken data de samlar in och för vilka syften. Företag ska inte få sälja vidare information till andra företag utan ditt uttryckliga medgivande. I dag får myndigheter lagra all information som inte uttryckligen är förbjuden. Vi anser att det borde vara förbjudet att lagra all information som inte är uttryckligen tillåten.
- ➔ Att en myndighet för integritetsskydd inrättas med ett samlat ansvar för skyddet av enskildas integritet.
- ➔ Att människor ska ha rätt att kontrollera sin persondata, exempelvis genom rätten att bli glömd. Det vill säga möjlighet att begära att sökmotorer som exempelvis Google tar bort resultat för sökfrågor som innehåller ens namn i fall resultaten är oriktiga, irrelevanta, eller överflödiga.
- ➔ Att ge möjlighet för Datainspektionen att utdöma kraftiga böter mot företag som bryter mot medborgares integritet samt ge möjlighet för medborgare att driva klagan mot företag och myndigheter som inte upprätthåller dataskyddet.
- ➔ Att integritetskränkande lagar såsom FRA, IPRED, PNR och Datalagringsdirektivet ska omförhandlas eller rivas upp.
- ➔ Att framtidens internet ska byggas på ett sätt som skapar bättre förutsättningar för integritet, där inbyggda mekanismer i IT-systemen fungerar som skydd för den personliga integriteten.

# KÄLLOR

---

European Parliamentary Research Service (2015) - **Review of the EU copyright Framework: European Implementation Assessment**

Engström & Falkvinge (2013) - **En reformerad upphovsrätt**

Renman Claesson (2011) - **Upphovsrätt : En annan ordning**

Karlsten (2013) - **Integriteten och samhällsutvecklingen**

Agrell (2015) - **Vem kan man lita på? den globala övervakningens framväxt**

Petterson & Agrell (2016) **Övervakning och integritet**

Alverén (2012) **Såld på nätet: priset du betalar för gratis**

Bylund (2013) **Personlig integritet på nätet**, Fores

Greenwald (2014) **No place to hide**

Wahlund mfl (2016) **Anseenderisker och dataskydd**, Stockholm School of Economics Institute for Research

Nakashima (2014-01-12) **NSA phone record collection does little to prevent terrorist attacks, group says**, The Washington Post

Kleja (2013-12-17) **PTS tar strid mot Säpos trafikdatakrav**, Ny Teknik

**Dataskyddsdirektivet, eller Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter**

**Datalag** (SFS 1974:289)

**Personuppgiftslag** (SFS 1998:239)

**Skyddet för den personliga integriteten – bedömningar och förslag**, Stockholm, 2008 (SOU 2008:3)

**Datalagring och integritet** (SOU 2015:31)

[www.datainspektionen.se](http://www.datainspektionen.se)

[www.dataskydd.net](http://www.dataskydd.net)



# KONTAKT

## Max Andersson, EU-parlamentariker

☎ Bryssel: +32 2 28 45457

Strasbourg: +33 3 88 175457

✉ max.andersson@ep.europa.eu

www www.maxandersson.eu

## Frida Johnson, politisk sekreterare

☎ + 46 70-988 48 55

✉ frida.johnson@ep.europa.eu



De Gröna | Europeiska fria alliansen  
i Europaparlamentet



## JA, JAG VILL...

- få mer information om Miljöpartiet de Gröna
- bli medlem i Miljöpartiet de Gröna
- bli medlem i Grön Ungdom (jag är under 26 år)
- bli medlem i Gröna Studenter

Namn: .....

Adress: .....

www.mp.se

porto

Miljöpartiet de Gröna  
Pustegränd 1-3  
118 20 Stockholm