Ny Juridik 4:09 s 40

Dataintrång

Författare: Henrik Bengtsson, Emil Dicksved

Den svenska lagstiftningen rörande dataintrång ändrades i juli 2007 som en anpassning till EU:s rambeslut om angrepp mot informationssystem och omfattar numera även s.k. denial-of-service-attacker och spridning av datorvirus. Advokat Henrik Bengtsson och jur. kand. Emil Dicksved vid Advokatfirman Delphi redogör för hur dataintrångsbestämmelsen har tolkats i domstolarna och var den svårbedömda gränsen för vad som är ett olovligt intrång dras. I artikeln behandlas även den rättsliga bedömningen vad avser olovligt utnyttjande av annans trådlösa datornätverk och bevisfrågor vid dataintrång.

Dataintrångsbrottet infördes i svensk rätt 1973. Antalet polisanmälningar som avser dataintrång har ökat ända sedan 1987 då åtta anmälningar gjordes (statistik före 1987 saknas). År 2008 gjordes 1 282 polisanmälningar. Den stora ökningen beror sannolikt på samhällets tilltagande datorisering, den kraftigt ökande Internetanvändningen samt att landsting, kommuner och myndigheter gått från fysiska aktmappar till dataregister, vilket ökat risken för olovlig tillgång till register. Dataintrång är således numera ett tämligen vanligt brott men tillämpningen av straffstadgandet har fått liten uppmärksamhet i doktrin.

Dataintrångsbestämmelsen har inte varit föremål för Högsta domstolens prövning men däremot finns det ett antal (refererade och orefererade) underrättsavgöranden där bestämmelsen prövats. Underrättsavgöranden måste naturligtvis analyseras kritiskt men illustrerar hur bestämmelsen tillämpas i praktiken.

Allmänt om dataintrång

Den handling som straffbelagts genom bestämmelsen om dataintrång i 4 kap. 9 c § brottsbalken är att någon (i) olovligen (ii) bereder sig tillgång till (iii) uppgift som är avsedd för automatiserad behandling eller olovligen (iv) ändrar, (v) utplånar, (vi) blockerar (vii) allvarligt hindrar eller stör, eller (viii) i register för in en sådan uppgift.

Olovlighetsrekvisitet

En förutsättning för straffansvar för dataintrång är, som ovan nämnts, att åtgärden sker *olovligen*. Åtgärder som vidtas i enlighet med lag faller inte under straffbudet. Åtgärder som vidtas med samtycke från den som disponerar över ett IT-system faller inte heller under straffbudet. Av förarbetena framgår att sedvanliga åtgärder som att testa ett systems säkerhet eller skydd, eller att installera nya program, som vidtas av behöriga personer inom behörigheten, inte är olovliga.

Beredande av tillgång till en uppgift kan ske olovligen genom att gärningsmannen kringgår säkerhetsåtgärder och knäcker eller utnyttjar lösenord (hackning) eller olovligen utnyttjar annans lösenord men även genom att gärningsmannen överträder behörighetsregler som uppställts i lag eller på annat vis. Lagstiftningen är vidare metodneutral och det uppställs inga krav på att gärningsmannen berett sig tillgång genom att kringgå någon säkerhetsåtgärd. Även kringgående av explicita eller implicita indirekta instruktioner omfattas av bestämmelsen.

Det krävs uppsåt i förhållande till olovligheten, vilket innebär att IT-systemets innehavares avsikt med hur IT-systemet får disponeras ska ha kommit till uttryck på ett sådant sätt att det är möjligt för en utomstående att uppfatta den.

Huruvida olovlighetsrekvisitet är uppfyllt ska avgöras efter en helhetsbedömning. Det saknas närmare kommentarer i förarbetena om hur tolkningen ska göras. Viss ledning bör kunna sökas i praxis rörande olovligt brukande och olovligt förfogande. Det ska dock noteras att bestämmelserna har olika tillämpningsområden eftersom olovligt brukande och olovligt förfogande i första hand avser brukande och förfogande av fysiska företeelser och inte uppgifter i en dator.

Ny Juridik 4:09 s 42

I praxis rörande olovligt brukande har användning av annans mobiltelefon - utan överenskommelse att telefonen fått nyttjas av gärningsmannen - för sändande av sms med delvis sexuellt innehåll ansetts utgöra olovligt brukande (Göta hovrätts dom i mål nr B 1087-07). Användning av arbetsgivares datorutrustning för att - utan samtycke - kopiera ett kundregister avsett för konkurrerande verksamhet har också ansetts falla under straffbudet (RH 2004:18). Olovlighetsrekvisitet i straffstadgandet olovligt brukande kan också vara uppfyllt om gärningsmannen fortsätter att utnyttja hyrd egendom efter att den avtalade hyrestiden gått ut (jämför NJA 1987 s. 388) eller utnyttjar arbetsgivarens egendom för privata ändamål (jämför NJA 1957 s. 337). Olovlighetsrekvisitet vid dataintrång torde mot denna bakgrund vara uppfyllt om en gärningsman bereder sig tillgång till en uppgift genom:

(i) brytande av säkerhetsspärrar,

(ii) överträdelser av behörighetsregler angivna i lag,

(iii) överträdelse av behörighetsregler uppställda av exempelvis arbetsgivare,

(iv) överträdelse av avtalsvillkor som reglerar behörighet avseende viss datorutrustning eller visst IT-system,

(v) fysiskt utnyttjande av annans datorutrustning utan samtycke.

Uppgiftsrekvisitet

Begreppet "uppgift som är avsedd för automatiserad behandling" innefattar alla uppgifter, dvs. fakta, information eller begrepp, som uttrycks i en för dator anpassad och läsbar form omfattas av bestämmelsen

(prop. 2006/07:66, s. 49). Uppgiftsbegreppet omfattar även datorprogram som sådana. Det saknar betydelse var i ett system uppgifterna lagras. Även uppgifter i en dators temporära minne och uppgifter som är under befordran omfattas av bestämmelsen oavsett på vilket sätt befordran sker (prop. 2006/07:66, s. 49). Uppgifter som befordras via radio omfattas endast då de är krypterade.

De otillåtna åtgärderna

Som nämnts ovan omfattas följande olovliga åtgärder av dataintrångs-bestämmelsen:

(i) *beredande av tillgång till en uppgift*Bestämmelsen innebär ingen begränsning avseende syftet med åtgärden att bereda sig otillåten tillgång, såsom att gärningsmannen avsett att insamla information eller att åstadkomma skada.

(ii) *ändring eller utplåning av uppgift*Bestämmelsen omfattar alla typer av ändringar och utplåningar i data.

(iii) *blockering av uppgift*Bestämmelsen gäller åtgärder som innebär att en uppgift görs oåtkomlig eller hindras från att flöda. Som exempel nämns i propositionen inmatning eller spridning av olika typer av sabotageprogram (t.ex. datavirus, trojaner eller logiska bomber) eller fyllande av minnesutrymmet hos en dator med skräpkod som medför att uppgifterna inte kan nås eller lokaliseras (prop. 2006/07:66, s. 50).

(iv) *införande av uppgift i register*Den del av bestämmelsen som avser olovligt införande i register har sitt ursprung i den numera upphävda bestämmelsen i 21 § datalagen. Eftersom begreppet härstammar från den numera upphävda datalagen ska begreppet sannolikt tolkas utifrån det registerbegrepp som gällde enligt densamma. Bestämmelsen skulle därmed omfatta endast införingar som sker i uppgifter strukturerade på visst sätt och som därmed kvalificerar sig som register.

(v) *allvarligt störande eller hindrande av användningen av en uppgift*Bestämmelsen avser åtgärder, som allvarligt stör eller hindrar användning av en uppgift, exempelvis genom tillgänglighets- eller överbelastningsattacker. Med "allvarligt störande eller hindrande" avses en betydande störning av inte endast tillfällig natur. Bedömningen av om en störning varit allvarlig ska göras utifrån en helhetsbedömning där faktorer såsom hur lång tid störningen pågått, störningens art och dess omfattning har betydelse. För ansvar förutsätts att gärningsmannen haft uppsåt att åstadkomma den störande eller hindrande effekten.

Cybercrimekonventionen och EU:s rambeslut om angrepp mot informationssystem

I november 2001 antog Europarådet "Convention on Cybercrime ETS no. 185", den s.k. Cybercrimekonventionen, en konvention om IT-relaterad brottslighet. Konventionen trädde i kraft den 1 juli 2004. Syftet med konventionen är att åstadkomma en harmonisering av straffrätten kring IT-relaterad brottslighet samt att effektivisera och underlätta arbetet mot IT-relaterad brottslighet över nationsgränserna.

I början av 2005 antogs rådets rambeslut 2005/222/RIF, även kallat EU:s rambeslut om angrepp mot informationssystem. Det bakomliggande syftet med rambeslutet var snarlikt syftet bakom Cybercrimekonventionen, nämligen att harmonisera den straffrättsliga lagstiftningen vad avser angrepp mot informationssystem t.ex. genom gemensamma definitioner, brottsrekvisit och påföljder inom unionen. Rambeslutet om angrepp mot informationssystem innehåller bl.a. bestämmelser om olagligt intrång i

informationssystem (Artikel 2) om olaglig datastörning (Artikel 4) om anstiftan, medhjälp och försök (Artikel 5) samt om påföljder och försvårande omständigheter (Artiklarna 6 och 7). Rambeslutets Artikel 2 punkt 1 stadgar att medlemsländerna ska vidta nödvändiga åtgärder för att straffbelägga uppsåtligt, orättmätigt, intrång i ett informationssystem, åtminstone i fall som inte är ringa. Enligt Artikel 4 i rambeslutet ska medlemsländerna straffbelägga uppsåtligt, orättmätigt, handlande som innebär att radera, skada, försämra, ändra, hindra flödet av eller göra det omöjligt att komma åt datorbehandlingsbara uppgifter i ett informationssystem, åtminstone i fall som inte är ringa.

2007 års ändringar i dataintrångsbestämmelsen

I samband med att datalagen (1973:289) år 1999 ersattes av personuppgiftslagen (1998:204) flyttades datalagens bestämmelse avseende dataintrång till brottsbalken utan att det innebar några egentliga ändringar i sak. I propositionen avseende angrepp mot informationssystem (prop. 2006/07:66) konstaterade regeringen att svensk rätt, genom dataintrångsbestämmelsen, uppfyllde rambeslutets krav på vad som ska vara straffbelagt som *olagligt intrång* i informationssystem. Däremot ansåg regeringen att det fanns vissa handlingar - som ska vara straffbelagda enligt EU:s rambeslut - men som ännu inte kriminaliserats i svensk rätt, nämligen DoS-attacker, virusangrepp och maskar.

I propositionen konstaterades att informationssystem är mycket sårbara mot angrepp, däribland olovliga intrång i informationssystem, samt störningar av sådana system och införande av falska eller felaktiga uppgifter i systemen. Virus och annan skadlig kod kan användas för att förstöra eller ändra uppgifter eller att avbryta eller hindra driften av informationssystem. En del virusprogram kan förorsaka skador på informationen i datorn, medan andra program utnyttjar datorn för att angripa andra datorer. Virusprogram kan vara sofistikerade och s.k. logiska bomber kan aktiveras genom en viss händelse, t.ex. att ett visst datum infaller, och då förstöra eller modifiera uppgifter. Andra program ("trojaner") utlöser angrepp när de öppnas. Ytterligare en typ av program ("datamaskar") kopierar sig själva. Kopiorna skapar sedan ännu fler kopior, vilket kan få till konsekvens att datorn ifråga till sist fylls av kopiorna. En annan form av sabotageåtgärd är s.k. tillgänglighetsattacker ("denial of service-attacker" eller "DoS-attacker") som blockerar eller sätter ned funktionen hos IT-system genom överbelastning. DoS-attacker kan ske genom en stor mängd upprepade anrop riktade mot ett IT-system men också genom program som sänder stora mängder e-post. Användandet av virusprogram och DoS-attacker omfattades inte av den äldre dataintrångsbestämmelsen.

I syfte att uppfylla rambeslutets krav justerades brottsbeskrivningen i 4 kap. 9 c § brottsbalken till att även omfatta olovlig *blockering* av en uppgift som är avsedd för automatiserad behandling (t.ex. genom spridning av olika typer av datavirus). Dataintrångsbestämmelsen

har också utökats med ett nytt led där det stadgas att även den som *olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift* ska dömas för dataintrång. Det nya ledet i bestämmelsen straffbelägger åtgärder som stör eller hindrar att uppgift kan användas på avsett sätt (t.ex. DoS-attacker).

I propositionen fastslog regeringen vidare att dataintrångs-bestämmelsen behövde moderniseras och förtydligas. Därför ersattes den tidigare bestämmelsens begrepp *upptagning för automatisk databehandling* med begreppet *uppgift som är avsedd för automatiserad behandling*. Justeringen genomfördes för att förtydliga att bestämmelsen också inkluderar uppgifter som utrycks i en för en dator anpassad och läsbar form, dvs.

fakta, information och begrepp. Detta innebär att även datorprogram av olika slag omfattas. Den nya ordalydelsen lämnar sålunda inget utrymme för diskussioner om vilken teknik som uppgifterna överförs med, på vilket datamedium uppgifterna förvaras eller om uppgifterna är "fixerade" eller inte. Avlyssning av uppgift som befordras via radio (radiokommunikation) faller fortfarande som huvudregel utanför det straffbara området.

Dataintrång - typfallen

Behörighetsöverskridande

Som nämnts ovan kan en anställd olovligen bereda sig tillgång till en upptagning genom att överträda en lagfäst behörighetsregel som anger vilka uppgifter den anställde har rätt att få tillgång till för fullgörande av sina tjänsteåligganden. I rättspraxis finns ett antal exempel på att sjukvårdspersonal, försäkringskassetjänstemän och poliser berett sig tillgång till uppgifter i annat syfte än att fullgöra sina arbetsuppgifter och har fällts till ansvar för dataintrång.

Behörighetsregler rörande åtkomst till data finns exempelvis i 4 § Rikspolisstyrelsens författningssamling 2005:8 Föreskrifter och allmänna råd om användning av IT-system inom Polisen, där det framgår att

IT-system som är tillgängliga inom Polisen får användas endast när det är nödvändigt för att genomföra en viss arbetsuppgift. Det ska vara sannolikt att användandet i det enskilda fallet är till nytta för arbetets genomförande.

På motsvarande vis finns det i patientdatalagen behörighetsregler som anger att

[d]en som arbetar hos en vårdgivare får ta del av dokumenterade uppgifter om en patient endast om han eller hon deltar i vården av patienten eller av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården (4 kap. 1 §),

respektive att

[e]n vårdgivare ska bestämma villkor för tilldelning av behörighet för åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat. Sådan behörighet ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården. (4 kap. 2 §).

Med "arbetsuppgift" avses i RPSFS 2005:8 tjänstemannens arbetsuppgifter inom ramen för sin ordinarie tjänst. En polis, som är verksam vid trafikenheten och som åtkommer uppgifter om en misstänkt misshandel, agerar således utanför ramen för sina arbetsuppgifter (jämför Södertörns tingsrätts mål nr B 13554-07). Registersökningar i syfte att lämna information ur Polisens spaningsregister till utomstående faller naturligtvis också utanför arbetsuppgiftsbegreppet (jämför Stockholms tingsrätts mål nr B 18144-07).

Personer, som varit arbetsbefriade under uppsägningstid och som berett sig tillgång till filer och e-post hos sin arbetsgivare, har också ansetts handla olovligen och har fällts till ansvar för dataintrång (se Mölndals tingsrätts mål nr B 893-05 respektive Stockholms tingsrätts mål nr B 2767-05). Före detta arbetstagares beredande av tillgång till arbetsgivarens IT-system efter anställningens upphörande har likaså betraktas som olovligt (se Uppsala tingsrätts mål nr B 3344-08).

Olovlighetsbedömningen har ställts på sin spets också i ett hovrättsmål, som rörde företagsspionerі och dataintrång (Hovrätten för Västra Sverige mål nr B 3146-04). Omständigheterna var att en anställd hade berett sig tillgång till företagshemlig information

från sin egen dator men också från två datorer som tillhörde personer i företagsledningen. Den tilltalade förklarade sitt handlande med att han hade haft problem med utskrifter och därför, som han uppfattade, anvisats att använda en annan dator. Mot bakgrund av att den anställde kunde anses ha fog för denna uppfattning och att det saknades åtkomstregler konstaterade hovrätten att den tilltalade inte haft uppsåt att olovligen bereda sig tillgång till uppgifterna, varför åtalet ogillades.

Sammanfattningsvis kan konstateras att domstolarna tillämpar en relativt sträng bedömning avseende behörighetsöverskridande och har ansett att den tilltalades utbildning eller förekomsten av åtkomstreglering i lag är tillräcklig för att den tilltalade ska ha uppsåt beträffande olovligheten. Även i situationer där det rimligen bör ha stått klart för den tilltalade att åtkomst inte var tillåten har subjektiv täckning ansetts föreligga avseende olovlighetsrekvisitet.

Det subjektiva rekvisitet och rättsvillfarelse

När det gäller uppsåtsbedömningen beträffande olovlighetsrekvisitet har Vänersborgs tingsrätt prövat ett mål (mål nr B 4487-04) där en läkare hade berett sig tillgång till patientjournaler vars vård läkaren inte hade del i. Läkaren hade vid ett tidigare tillfälle blivit tillsagd att tillgången var otillåten och han ansågs därför ha kunskap om att åtkomsten var olovlig. Solna tingsrätt har i ett mål (mål nr B 6095-08) som gällde en läkares åtkomst till patientdata ansett att läkaren genom sin utbildning måste anses ha insett att åtkomst till uppgifter avseende patienter för vilka läkaren inte har vårdansvar inte är tillåtet.

I RH 2002:36 friade Hovrätten för Västra Sverige en sjuksköterska, som hade berett sig tillgång till den avlidne dåvarande invandrarministerns Leif Blombergs patientjournal, trots att hon inte ingick i den krets som behövde ta del av journalen som ett led i vårdarbetet. Sjuksköterskan hade arbetat inom sjukvården i trettio år och hade fått utbildning om patientjournallagen och dess bestämmelser. Sjuksköterskan menade att hon, i och med att patientjournalerna började digitaliseras i mitten av 1990-talet, fått uppfattningen att journalreglerna hade ändrats. Hon uppgav också att det i samband med digitaliseringen av patientjournalerna även skulle antecknas omvårdnadsplaner i journalen (information

som tidigare bara förts vidare muntligt och vid digitaliseringen överläts den praktiska hanteringen till sjuksköterskorna). Sjuksköterskan uppgav att det blev vanligt förekommande att sjuksköterskor som ett stöd i journalarbetet även tog del av sådana journaler, som hörde till andra än de patienter som de aktivt deltog i vården av. Vissa sköterskor blev till och med tillsagda att gå in i olika patientjournaler i syfte att jämföra och se hur korrekt dokumentationen skulle se ut. Sjuksköterskan blev dock aldrig själv direkt uppmanad att göra detta. Hon ville se hur dokumentation fördes och tittade först i en patients journal men hittade inte vad hon letade efter och öppnade av en slump även Blombergs journal. Hovrätten konstaterade att en person som bereder sig tillgång till en patientjournal, utan att ingå i den krets som behöver ta del av den aktuella journalen för vårdarbetet, objektivt gör sig skyldig till dataintrång, även om huvudsyftet varit att leta efter lämpliga skrivningar för det egna journalförandet. Hovrätten ansåg vidare att över 30 personer tagit del av den aktuella journalen utan att detta var ett led i vårdarbetet och att det var ytterst sannolikt att de flesta gjort detta av ren nyfikenhet. Hovrätten godtog dock sjuksköterskans påstående om att hon inte hade vetskap om att hennes agerande var otillåtet. Hovrätten menade vidare att straffrättsvillfarelse (24 kap. 9 § brottsbalken), i de fall villfarelsen är

uppenbart ursäktlig, kan medföra straffrihet och att det är endast vid lindrig brottslighet som man kan överväga att med hänvisning till bestämmelsen fria från ansvar. Hovrätten bedömde sjuksköterskans dataintrång som ett lindrigt brott eftersom syftet med intrånget var att söka efter lämpliga formuleringar för eget journalskrivande. Eftersom det fanns stöd för att det bland vissa läkare och annan personal fanns en felaktig uppfattning att det var acceptabelt att gå in och ta del av främmande patientjournaler i utbildningssyfte och att detta även hade förekommit ansåg hovrätten att sjuksköterskan, som haft en relativt underordnad ställning i organisationen, varit ovetandes om det otillåtliga i hennes agerande och därigenom skulle gå fri från ansvar.

I ett annat mål (mål nr B 7095-02) prövade Svea hovrätt huruvida en socialsekreterare, som vid omkring 65 tillfällen använt socialförvaltningens klientregister för privata intressen, skulle dömas till ansvar för dataintrång eller inte. Utredningen i målet visade att det inte fanns några skriftliga direktiv om när en

tjänsteman hade rätt att gå in i en klients dataakt. Hovrätten uttalade dock att socialsekreteraren på grund av sitt arbete och sin socionomutbildning måste ha insett att hon inte hade rätt att utom tjänsteutövningen och av privata skäl ta del av sekretessbelagda uppgifter i datasystemet och att hon därför med uppsåt handlat olovligen. I ett mål vid tingsrätten i Borås (mål nr B 127-09) var en läkare åtalad för att obehörigen tagit del av känsliga uppgifter i en patientjournal. Tingsrätten konstaterade att det vid den aktuella kliniken inte funnits någon tvekan om vad som var tillåten respektive otillåten läsning av patientjournaler. Tingsrätten fastslog att syftet med läkarens läsning av patientjournalen var nyfikenhet och att handlandet inte kunde föranleda frihet från straffansvar på grundval av straffrättsvillfarelse.

Mot bakgrund av ovanstående redogörelse kan det konstateras att domstolarna i underrättspraxis tillämpat olovlighetsrekvisitet och straffrihet p.g.a. straffrättsvillfarelse något olika. Artikelförfattarna ifrågasätter om inte hovrätten i det ovan redovisade rättsfallet skulle konstaterat att det på det aktuella sjukhuset vid tidpunkten hade utvecklats en praxis som tillät att sjuksköterskor i utbildningssyfte tog del av andra patienters journaler. I stället för att fria sjuksköterskan på grund av straffrättsvillfarelse kunde hennes handlande bedömts som lovligt, vilket hade inneburit att olovlighetsrekvisitet inte hade varit uppfyllt.

Missbruk och ändring av lösenord

Även missbruk och ändring av annans lösenord utgör som ovan nämnts dataintrång. Det finns flera sätt på vilka en person olovligen kan komma över annans lösenord. Personen kan t.ex. genom att använda ord från en ordlista testa olika ordkombinationer för att gissa sig fram till ett lösenord, en s.k. *brute-force-attack*. Det är inte heller ovanligt att personer utger sig för att vara legitima användare av ett datasystem och på så sätt manipulerar andra användare till att avslöja lösenord eller annan säkerhetsrelaterad information, s.k. *social engineering* (en variant av detta är s.k. nätfiske eller *phishing* som ofta förekommer vid bankbedrägerier på Internet). Även säkerhetsbrister i ett system kan utnyttjas för att åtkomma lösenord.

Lunds tingsrätt (mål nr B 4520-07) fällde en man för grovt bedrägeri medelst dataintrång sedan han under ett antal chattkonversationer

låtsats vara en minderårig flicka som skulle sälja en show genom web-cam och förmått dem han chattat med att ladda hem en nakenbild på den unga flicka han utgav sig för att vara. Till bilden hade fogats en fil med ett fjärrstyrningsprogram som gjorde det möjligt för honom att ta sig in i de aktuella personernas datorer och kopiera certifikat och lösenord som möjliggjorde att på olika sätt genomföra köp och överföra pengar till olika bankkonton.

I det i media mycket uppmärksammade rättsfallet rörande intrång i Socialdemokraternas datorsystem inför valet 2006 fällde Stockholms tingsrätt (mål nr B 19611-06) en journalist för dataintrång. Journalisten hade loggat in på Socialdemokraternas interna nätverk Sapnet med inloggningsuppgifter han fått från den dåvarande pressekreteraren i Liberala ungdomsförbundet. Uppgifterna hade denne i sin tur fått från SSU:s dåvarande ombudsman. Ombudsmannen hade kommit över inloggningsuppgifterna då han hjälpt en medarbetare med dennes e-post. Även den dåvarande pressekreteraren och ombudsmannen befanns skyldiga till dataintrång.

I ett mål från Karlskoga tingsrätt (mål nr B 346-07) dömdes en man för bedrägeri och dataintrång då han olovligen berett sig tillgång till annans hotmail-konto genom att använda dennes lösenord och användarnamn. Därefter hade intrångsgöraren ändrat hotmail-lösenordet och skaffat sig tillgång till inloggningsuppgifter för ett Internetbaserat pokerkonto på vilket han loggat in och på så sätt olovligen disponerat över målsägandens tillgångar.

I ett annat rättsfall (RH 2004:40) dömde Göta hovrätt en man för såväl dataintrång som sexuellt ofredande efter att han olovligen berett sig tillgång till ett Lunarstormkonto och ändrat profilen genom att svara förnedrande på de 20 frågor som beskrev användaren. Frågan om missbruk eller ändring av lösenord innebär i allmänhet inte några svårare juridiska bedömningar.

Virusspridning och DNS-attacker

Frågan om spridning av virus har redan kommit att prövas av domstolarna. I ett avgörande från Svea hovrätt (mål nr B 1819-07) fälldes en man för dataintrång efter att han via en dator på Chalmers tekniska högskola loggat in på ett användarkonto och lagt in en modifierad programvara, som gjorde det möjligt för honom att erhålla fler inloggningsuppgifter. Programvaran använde

han sedan för att ta sig vidare in i andra system. Gärningsmannen hade även skapat dolda mappar och installerat programvara i syfte att dölja sin identitet. Tingsrätten friade mannen som menade att det var någon annan som begått intrången via hans användarkonton. Hovrätten konstaterade dock att gärningsmannen måste varit mycket säkerhetsmedveten eftersom han, enligt egen utsago, till och med loggade vad hans kamrater gjorde på servern. Mot bakgrund av hans säkerhetsmedvetenhet framstod det som mycket osannolikt att han skulle ha upplåtit konton till olika hackare utan att ha kontroll över vad dessa gjorde på servern. Hovrätten dömde därför den tilltalade för dataintrång. Målet överklagades till Högsta domstolen, som inte meddelade prövningstillstånd.

I ett mål från Ångermanlands tingsrätt (mål nr B 622-03), (målet har överklagats till Hovrätten för Nedre Norrland, mål nr B 1258-07, men inte prövats vid manusläggning) fälldes en man för dataintrång och egenmäktigt förfarande då han hade programmerat och skickat en s.k. e-postmask. Ett program som hade bifogats e-postmeddelandet som användaren uppfattade innehålla ett skärmsläckarprogram. Programmet innehöll dock en mask som efter installation letade igenom den angripna datorn efter e-postadresser och som spred sig sedan själv vidare genom massutskick till de e-postadresser som masken hittat. Den tilltalade menade att han inte insett att masken skulle sprida sig så fort och i så stor omfattning som den gjort. Han påstod att han inte visste att människor hade så många e-postadresser i sina datorer. Tingsrätten konstaterade att de objektiva rekvisiten för dataintrång uppfyllts eftersom mannen, genom att programmera och skicka ut masken, i ett mycket stort antal register olovligen ändrat och fört in programkod i upptagningar för automatisk databehandling. Tingsrätten menade vidare att mannen gjort sig skyldig till egenmäktigt förfarande då massutskicken av masken lett till "e-postbombning" av bland annat Tidningen Ångermanland, Aftonbladet och SVT samt att dessa företags DNS-servrar inte kunnat användas på avsett vis. Enligt tingsrättens bedömning utgjorde detta en sådan besittningsrubbning som omfattas av straffstadgandet egenmäktigt förfarande. Tingsrätten ansåg att mannen var medveten om att mottagaren av e-posten skulle få sin dator smittad och att

han även varit medveten om att masken var programmerad att skicka sig själv vidare. Gärningsmannen fälldes därför till ansvar.

Sammanfattningsvis kan konstateras att de två avgöranden, som rör spridning av virus och DNS-attacker, har varit tekniskt komplicerade fall vilka innehållit svåra bevisfrågor. Detta ställer naturligtvis stora krav på teknisk kunskap hos såväl åklagare och försvarare som domstol. Det är ett faktum att antalet spridda virus och DNS-attacker ökar men att endast ett fåtal fall leder till åtal, vilket sannolikt beror på de tekniska svårigheterna att finna gärningsmannen och att visa att denne begått ett uppsåtligt brott.

Olovlig tillgång till trådlöst nätverk?

Trådlösa datornätverk förekommer numera frekvent och det är inte ovanligt att innehavaren av ett sådant nätverk inte har aktiverat åtkomstkontroll av detsamma, dvs. ett skydd mot att obehöriga bereder sig tillgång till nätverket. Frågan om hur användningen av annans skyddade eller oskyddade trådlösa nätverk ska bedömas har oss veterligen inte aktualiserats i domstolarnas praxis. Som framgått ovan är olovligt beredande av tillgång till data att bedöma som dataintrång under förutsättning att gärningsmannen berett sig tillgång till "en upptagning för automatisk databehandling" med vilket avses en upptagning för automatisk databehandling, som är fixerad på någon form av datamedium och som alltså antingen finns i eller kan matas in i en dator.

I promemorian Brott och brottsutredning i IT-miljö (Ds 2005:6 s. 215) föreslogs att dataintrångsbestämmelsen skulle ändras så att den skulle omfatta även den som 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. När promemorian sedermera resulterade i en proposition föreslogs dock inget avlyssningsbrott som en del av dataintrångsbestämmelsen. Regeringen konstaterade att bestämmelsen i och för sig ger ett skydd för uppgifter under befordran men att det för straffansvar förutsätts att gärningen är olovlig. Eftersom etern är fri är avlyssning av trådlösa datorkommunikationer i princip inte olovligt vilket innebär att dataintrångsbestämmelsen inte är tillämplig på intrång i okrypterade radiobefordrade uppgifter (prop. 2006/07:66, s. 41). Däremot menade regeringen att dataintrångsbestämmelsen kan vara tillämplig på andra typer av angrepp som t.ex. ändring eller radering av uppgifter som befordras

via radio.

Åtkomst till annans öppna trådlösa nätverk torde heller inte falla under avlyssningsförbudet i lagen om elektronisk kommunikation eftersom lagen bygger på att principen att etern är fri och det kan därför inte anses otillåtet att avlyssna ett annat trådlöst nät som någon fått automatisk tillgång till (6 kap. 17 §, 3 p.).

Post- och Telestyrelsen ansåg i sin promemoria *Säkerhet i lokala trådlösa nät* att beredandet av tillgång till trådlös datorkommunikation kan betraktas som olovligt brukande enligt 10 kap. 7 § brottsbalken. Olovlig användning av annans IT-utrustning kan i och för sig utgöra olovligt brukande (jämför RH 2004:18) men mot bakgrund av den tydliga principen om eterns frihet kan det, som konstaterats ovan, ifrågasättas om beredande av tillgång till annans trådlösa nätverk över huvud taget kan vara olovligt. Därtill kommer att olovligt brukande för att falla under straffstadgandet ska ha förorsakat "skada eller olägenhet". I teorin skulle innehavaren av en Internetuppkoppling kunna drabbas av skada eller olägenhet genom att uppkopplingshastigheten blir lägre till följd av ökat nyttjande men det förefaller tveksamt om denna skada eller olägenhet skulle vara sådan att straffstadgandet blir tillämpligt. Däremot är det tänkbart att skada eller olägenhet snarare skulle kunna vara att den som olovligen brukar nätverket gör sig skyldig till ett lagbrott på nätet (t.ex. upphovsrättsintrång eller

barnpornografi) och på så sätt gör att abonnenten felaktigt blir misstänkt för den brottsliga gärningen. Eftersom en dator, beroende på inställningar, automatiskt kan ansluta till öppna trådlösa nätverk kan datoranvändaren i många fall sakna uppsåt i förhållande till olovligheten och därmed inte fällas till ansvar för olovligt brukande. Det kan också diskuteras huruvida den som tillhandahåller ett öppet trådlöst nätverk lämnat ett underförstått samtycke för andra personer att använda Internetuppkopplingen, i vilket fall olovlighetsrekvisitet inte heller skulle vara uppfyllt.

Bevisfrågor

Liksom i övriga mål som rör brott begångna med hjälp av datorer eller IT-utrustning uppstår det i dataintrångsmålen relativt svåra bevisfrågor när det gäller huruvida information åtkommits och vem som använt sig av en viss dator och ett visst IP-nummer vid en viss tidpunkt.

I ett rättsfall från Hovrätten över Skåne och Blekinge (RH 2000:90) invände den tilltalade, en polis som gjort slagningar i polisens register utan att detta behövts för fullgörandet av hans arbetsuppgifter, att han - trots registersökningarna - inte fått tillgång till några uppgifter, varken genom utskrift eller i form av information på skärmen. Hovrätten konstaterade dock att möjligheten att i efterhand säkra bevis om vilken information som en person som olovligen berett sig tillgång till ett register verkligen tagit del av är mycket begränsade. Hovrätten konkluderade därför att i bevishänseende kan ett sådant påstående godtas endast om det stöds av andra omständigheter. Sådana omständigheter fanns inte i det aktuella fallet, varför polisen dömdes för dataintrång.

Det har också visat sig att en vanlig invändning från den tilltalade är att denne tillhandahållit ett trådlöst datornätverk, som varit tillgängligt för envar och att det därför kan vara någon annan som vidtagit gärningen. De frågor som aktualiseras i detta sammanhang är vem som vid tidpunkten för lagöverträdelsen:

(i) använde datorn?

(ii) använde den aktuella Internetuppkopplingen?

Dessa frågor har kommit att bedömas av underrätterna i dataintrångsmål, upphovsrättsintrångsmål och förtalsmål, där brotten förövats på Internet eller i annan IT-miljö. Vid ett studium av dessa domar kan konstateras att landets tingsrätter och hovrätter har en divergerande syn på den tilltalades invändning om att någon annan kan ha använt den aktuella datorn eller IP-numret för att begå brott.

I ett uppmärksammat upphovsrättsintrångsmål (mål nr B 8799-05), som rörde olovlig fildelning av filmen "Hipp Hipp Hora", invände den tilltalade att den IP-adress från vilket filmen tillgängliggjorts inte kunde kopplas till den tilltalades Internetabonnemang. Svea hovrätt gjorde en ingående prövning av vid vilken tidpunkt filmen ifråga gjordes tillgänglig och gjorde följande principiella uttalande i frågan om vilket beviskrav som ska ställas i detta sammanhang:

För att [den tilltalade] skall kunna ådömas ansvar för den gärning som åklagaren har lagt honom 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.

Hovrätten menade således att det utifrån bevisningen inte gick att dra någon säker slutsats om när filmen hade överförts eller om överföringen gjorts från den tilltalades dator. I ett senare avgörande från Borås tingsrätt (domslutet fastställdes av Hovrätten för Västra Sverige, mål nr B 4465-06) hänvisade tingsrätten till Svea hovrätts ovan nämnda beviskrav men ansåg att det inte förekommit något som talade för att någon annan använt den tilltalades Internetuppkoppling. Linköpings tingsrätt ansåg vidare i ett fildelningsmål (mål nr B 1066-06) att ett så strängt beviskrav som att det ska vara uteslutet att någon annan använt sig av utrustningen inte borde uppställas och lämnade allmänt hållna uppgifter om att någon annan kunde ha använt sig av den tilltalades router utan avseende. I målen i Borås och Linköpings tingsrätter hade dock de tilltalade lämnat uppgifter i polisförhör som lades till grund för tingsrätternas slutsatser att ingen annan utnyttjat utrustningen. Frågan har också aktualiserats i dataintrångsmål där Växjö tingsrätt (mål nr B 1874-08) tillämpat det strängare beviskravet, men ansett att det varit uteslutet att någon utomstående använt den tilltalades Internetuppkoppling. Nacka tingsrätt (mål nr B 565-02) har ansett att det mot den tilltalades bestridande inte kunde anses styrkt att inte någon annan olovligen hade berett sig tillgång till ett Internetkonto och har friat den tilltalade. Stockholms tingsrätt har dock i ett mål rörande dataintrång i en webbplats (mål nr B 145-07) ansett att ett alternativt händelseförlopp, innebärande att någon annan person skulle ha loggat in på ett användarkonto från den tilltalades IP-adress, inte framstod som sannolikt.

Det framstår som olyckligt att domstolarna tillämpar olika beviskrav i frågan om vem som har begått en gärning med hjälp av en viss dator eller Internetuppkoppling. Det kan naturligtvis finnas ett flertal anledningar till tvivel huruvida en innehavare av ett visst Internetabonnemang har vidtagit en viss åtgärd, abonnenten kan ha ett öppet trådlöst nätverk, någon annan kan ha haft fysisk tillgång till datorn eller gjort intrång i datorn med hjälp av trojanska hästar eller virus. Lunds tingsrätt friade den tilltalade i ett barnpornografimål (mål nr B 2208-99) just på den grunden att

filer kunde ha laddats ned av någon annan, som gjort dataintrång. Det av Svea hovrätt uppställda beviskravet, att det ska vara uteslutet att någon annan använt den aktuella datorn eller Internetabonnemanget, innebär att utrustning för trådlösa nätverk såsom router i princip alltid måste analyseras för att fastställa om någon annan vid tidpunkten för den misstänkta gärningen haft tillgång till Internetuppkopplingen (jämför Westman, Daniel *Bevisfrågor vid upphovsrättsintrång genom fildelning* m.m., Lov & Data nr 88 december 2006, s. 36-39).

Frågan är om det gängse beviskravet i brottmål, nämligen att det ska vara ställt utom allt rimligt tvivel att den tilltalade begått gärningen, ska tolkas så att alternativförklaringar måste, såsom Svea hovrätt anfört, vara *uteslutna*. Det förefaller märkligt att tillämpa ett särskilt högt beviskrav på grund av att datorer eller IT-utrustning används vid förövandet av ett brott.

Dataintrång - svårbedömda olovlighetsfrågor

Internetrelaterade frågor m.m.

Ett intressant beslut från sjätte Åklagarkammaren i Stockholm (Dnr C06-5-3688-02) avsåg en polisanmälan om dataintrång. Anmälan gjordes av programvaruföretaget Intentia som avsåg att publicera sin kvartalsrapport på sin webbplats vid ett visst klockslag. För att underlätta publiceringen lade man upp filen med kvartalsrapporten under länken på servern några timmar före den planerade publiceringen, men utan att några länkar fanns till filen från Intentias webbplats. Länkningen skulle läggas upp först vid det planerade klockslaget. Nyhetsbyrån Reuters gick emellertid ut med information om rapportens innehåll en timme innan publiceringen skulle äga rum. Vid en granskning av loggarna visade det sig att en dator från Reuters hade åtkommit rapporten kort efter det att den laddats upp på servern. Reuters reportrar hade nämligen gissat sig till den exakta adressen för

kvartalsrapporten genom att använda samma adressmönster som använts för företagets tidigare kvartalsrapporter och att byta ut "Q2" mot "Q3" i adressen. Åklagaren, som beslutade att lägga ned förundersökningen, konstaterade att gärningen dataintrång förutsätter att någon olovligen berett sig tillgång till en upptagning för automatisk databehandling men att

det inte ställs några krav på att gärningsmannen t.ex. knäcker ett lösenord eller dekrypterar en fil. Åklagaren konstaterade vidare att det för straffansvar krävs

att systeminnehavarens avsikt om vad som är lovligt eller inte kommit till uttryck på ett sådant sätt att det är möjligt för en utomstående att uppfatta den.

Intentia menade att deras avsikt varit tydlig eftersom bolaget gått ut med information om att kvartalsrapporten skulle publiceras vid ett visst klockslag, inte tidigare. Åklagaren ansåg dock att det måste vara allmänt känt att man kan komma åt en publik webbplats genom att ange dess fullständiga sökväg i en webbläsare och att många användare förkortar tiden för återsökning av information genom att skriva in hela sökvägen i stället för att ta sig fram via länkar från en startsida. Åklagaren menade också att det inte är ovanligt att man får kännedom om en sådan sökväg från en bekant. Därmed fanns det enligt åklagaren en reell möjlighet att avsaknaden av länkar från startsidan inte uppmärksammas av användaren. Mot denna bakgrund menade åklagaren att avsaknaden av länkar till kvartalsrapporten från Intentias startsida och det faktum att rapporten skulle publiceras omkring klockan 14.00 inte kunde anses göra en uppfattningsbar begränsning av rapportens tillgänglighet. Förundersökningen lades därför ned eftersom Reuters anställda inte kunde antas ha insett att tillgängligheten var begränsad.

Åklagarens beslut är intressant eftersom det faktum att åtkomsten inte var olovlig kopplas så tydligt till den tidpunkt då rapporten skulle publiceras. Frågan om olovlig beredande tillgång kunde ha avfärdats redan på den grunden att det inte kunde anses olovligt att ändra delar av en Internetadress för att underlätta navigering. Något svar på om Internetnavigering genom manuella ändringar av adressen skulle kunna utgöra dataintrång finns därför inte.

Det finns även andra tänkbara situationer då det kan vara svårt att visa att ägarens avsikt om vad som är lovligt eller inte kommit till uttryck på ett sådant sätt att det är möjligt för en utomstående att uppfatta det. Om en användare av en publik dator med tillgång till Internet får tillgång till webbsidor där en tidigare användare sparat lösenord kan det diskuteras om tillgången till en sådan webbsida utgör dataintrång. Om någon finner ett borttappat portabelt

minne (exempelvis USB-minne) och öppnar detta minne på en dator kan det likaså diskuteras om öppnandet sker lovligen eller ej. Ytterligare exempel på när dataintrångsbrottet skulle kunna aktualiseras är om ett uppenbart feladresserat e-brev eller ett ebrev som innehåller en bilaga som av dess titel att döma inte är avsedd för mottagaren öppnas av mottagaren. Det kan i dessa fall diskuteras huruvida avsändarens avsikt att begränsa rätten att ta del av innehållet kommit till uttryck och således om ett öppnande kan betraktas som olovligt. Nämnda exempel belyser det faktum att dataintrångsbestämmelsen formulerats som en generalklausul med ett potentiellt mycket vitt tillämpningsområde där just olovlighetsrekvisitet och gärningsmannens uppsåt avseende olovligheten kan vara mycket svårbedömda.

Anställdas privata filer

En fråga som flera gånger varit föremål för utredning (se bl.a. SOU 1992:110 Datastraffrättsutredningen, SOU 2002:18 Personlig integritet i arbetslivet och SOU 2009:44 Integritet i arbetslivet) men som inte fått något definitivt svar, är frågan om arbetsgivaren får bereda sig tillgång till anställdas filer eller e-post, som sparats i mappar märkta "privat" eller liknande. Eftersom arbetsgivaren i normalfallet äger eller leasar IT-utrustningen har arbetsgivaren tillgång till den utrustning där de privata filerna finns lagrade. Arbetsgivaren har därför rätt att förfoga över utrustningen som sådan och kan utan särskilda åtgärder komma åt information i systemet även om den skyddas av lösenord. Den rättsliga frågan är om arbetsgivarens de facto tillgång också innebär att arbetsgivaren har *lovlig* rätt att bereda sig tillgång till filer eller e-post av privat natur.

Om arbetsgivaren har utfärdat riktlinjer för i vilken omfattning han eller hon får ta del av information och sedan avviker från sina egna riktlinjer, ansåg Integritetsutredningen att förfarandet torde vara att betrakta som olovligt (SOU 2002:18 s. 113). Datastraffrättsutredningen menade att om en arbetsgivare klart har gett till känna att informationsbehandling inte får ske för privata ändamål har han också rätt att bereda sig tillgång till data, vilka förvaras i de datautrymmen han tillhandahåller, som behövs för att kontrollera om så sker. Om arbetstagaren däremot fått rätt att använda utrustningen utanför arbetet ansåg Datastraffrättsutredningen att

arbetsgivaren inte fick bereda sig tillgång till dessa datautrymmen (SOU 1992:110 s. 560). Utredningen föreslog vidare en restriktiv hållning vid oklara förhållanden när det gäller bestämmandet av i vilken omfattning anläggningens innehavare får bereda sig tillgång till användarnas data. Integritetsutredningen stannade dock vid att frågan i avsaknad av domstolspraxis var oklar. Sören Öman har i *Privat e-post på arbetet* i Festskrift till Reinhold Fahlbeck kommenterat frågeställningen och ansett att det är olovligt för arbetsgivaren att ta del av arbetstagares e-post i strid dels med de uttryckliga avtal eller riktlinjer arbetsgivaren har ingått eller utfärdat i fråga om att ta del av e-post, dels med god sed på arbetsmarknaden, men att det i övrigt är lovligt att göra det.

Mot bakgrund av den osäkerhet som gäller beträffande denna fråga kan det dock ifrågasättas om en arbetsgivare som, utan uttryckligt medgivande från den anställde, bereder sig tillgång till den anställdes privata filer eller e-postmeddelanden kan anses ha uppsåt i förhållande till olovlighetsrekvisitet.

Slutord

Av redogörelsen ovan framgår att dataintrång kan begås genom att någon olovligen bereder sig tillgång till en uppgift. Huruvida en åtkomsthandling omfattas av straffbudet kommer, i de fall som inte avser uppenbar hackning eller användande av annans lösenord, att avgöras på grundval av huruvida gärningsmannen olovligen har berett sig tillgång till uppgiften eller ej och om gärningsmannen haft uppsåt i förhållande till olovlighetsrekvisitet. Eftersom olovlighetsrekvisitet omfattar situationer där gärningsmannen inte bara insett utan också rimligen bort inse att innehavaren av datorsystemet uppställt en behörighetsbegränsning får bestämmelsen ett mycket vitt tillämpningsområde och handlingar som måhända inte uppfattas som lagstridiga riskerar att omfattas av straffbudet. Då det inte uppställs något krav på att innehavaren av datorsystemet uttryckligen uppställt behörighetsregler eller vidtagit säkerhetsåtgärder finns det risk för att dataintrångsbestämmelsen blir en svårförutsägbar bestämmelse av generalklausulskaraktär, vilket skapar rättsosäkerhet. Dessutom saknas det vägledande avgöranden från Högsta domstolen om hur olovlighetsrekvisitet och gärningsmannens insikt om och uppsåt i förhållande till olovligheten ska tolkas.

Av Cybercrimekonventionen (Artikel 3) och Rambeslutet rörande angrepp på informationssystem (Artikel 2) följer att konventions- respektive medlemsstaterna får besluta att olagligt intrång ska kriminaliseras endast när

brottet begås genom intrång i en säkerhetsåtgärd. Eftersom den svenska bestämmelsen inte bygger på denna förutsättning får svensk straffrätt ett vidare tillämpningsområde än i vissa andra länder. Ur ett rättssäkerhetsperspektiv kan det dock ifrågasättas om handlanden såsom i de exempel som nämnts ovan under rubriken Dataintrång - svårbedömda olovlighetsfrågor vars olovlighet kan vara mycket svårbedömda, ska omfattas av straffbudet.