Krav til informationssikkerhed

Af **Peter Blume,** Jura, KU

Studerende Christina Jensen går i banken for at hæve et beløb på sin bankkonto. Til sin forfærdelse opdager hun, at kontoen er lænset og står i minus. En anden person har muntret sig med at hæve penge og købe ind i hendes navn – ved brug af hendes CPR- og bankkonto-nummer. Et glemt sygesikringsbevis og bankens sløseri med at kræve fuld legitimation er årsag til hele miseren. Lis har været udsat for identitetstyveri.

Identitetstyveri er blot en af de mange nye trusler mod informationssikkerheden, som er opstået i kølvandet af digitaliseringen i samfundet. Hvor der er mulighed for at skaffe sig lette penge på andres bekostning, vil der altid være personer, der forsøger at snyde systemet. Og har held med det, fordi der ikke findes en 100% sikker metode til at garantere informationssikkerheden.

It- eller informationssikkerhed er et komplekst område, som der ikke bare findes en enkelt, men derimod en række forskellige metoder og tilgange til. Ingen af dem kan stå alene – de må supplere hinanden.

Lovgivningen indeholder regler og retningslinjer, som både private virksomheder og organisationer og offentlige myndigheder med ansvar for egne og andres data skal kende og efterleve. Derudover handler it-sikkerhed især om fornuftig adfærd og om at tage teknikken til hjælp.

Denne artikel giver først en grundig indføring i reglerne ved professor dr.jur. Peter Blume – og suppleres med en faktaboks med en liste over de mest typiske sikkerhedstrusler.

Hvordan kan du være sikker på, at offentlige myndigheder og private virksomheder ikke misbruger oplysninger om dig? Kan du være sikker på, at ingen andre får adgang til oplysningerne? Svaret på disse spørgsmål findes i loven om behandling af personoplysninger, som bl.a. stiller krav til offentlige myndigheders og private virksomheders informationssikkerhed. Artiklen beskriver, hvilke krav der stilles til informationssikkerhed i dag og i fremtiden.

Hvorfor bekymre sig om informationssikkerheden?

I informationssamfundet spiller oplysninger om personer en væsentlig rolle. Det kan fx være oplysninger om kunderne i en virksomhed eller kommunens oplysninger om borgernes indtægter. Sådanne oplysninger kaldes i lovgivningen for personoplysninger.

Når en offentlig myndighed eller en privat virksomhed opretter et register med personoplysninger, kan de bruge oplysningerne til mange nyttige formål, som sikrer, at borgerne og kunderne får en god, hurtig og effektiv behandling. Der er dog altid en risiko for, at personoplysningerne kan bruges til formål, som den enkelte person ikke ønsker, eller som er ulovlige. Eller endnu værre: at personer uden for myndigheden eller virksomheden kan få adgang til fortrolige personoplys-

ninger. For at sikre borgerne mod misbrug af persondata har man i Danmark og i en række andre lande vedtaget regler om databeskyttelse og informationssikkerhed. I Danmark står reglerne i "lov om behandling af persondata", også kendt som "persondataloven".

Hovedformålet med reglerne er at undgå, at personoplysninger misbruges – med den konsekvens, at den enkelte persons integritet og privatliv krænkes. Risikoen herfor kan opstå i et utal af situationer. Som eksempler kan nævnes misbrug af CPR-numre og passwords med det formål at lænse bankkonti, hacking af hjemmesider eller udstilling af personers portrætter på hjemmesider.

Informationssikkerhed er en fundamental del af informationssamfundet, fordi reglerne om sikkerhed har stor betydning for den tillid, som informationsteknologien mødes med. Spørgsmålet er bare, hvordan man sikrer, at reglerne fungerer efter hensigten, således at der er tale om en reel sikkerhed. Som hovedregel skal det sikres, at personoplysninger kun anvendes af autoriserede personer til autoriserede formål. Dette er en forudsætning for, at borgerne kan have ikke blot tillid til systemerne, men også tryghed, fordi brugen af teknologien bliver mere gennemskuelig for den enkelte.

Hvad siger persondataloven om informationssikkerhed?

Persondataloven har en regel om informationssikkerhed i § 41, stk. 3, som fastslår, at "Den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for databehandlere."

Persondataloven indeholder de grundlæggende regler om de sikkerhedskrav, der skal være opfyldt, når man anvender personoplysninger. Selvom der også i andre sammenhænge gælder regler om sikkerhed, er det først og fremmest i forhold til personoplysninger, at sådanne krav er aktuelle, og det er derfor beskyttelsen af personoplysninger, der er temaet i denne artikel. Det er de skadevirkninger for borgerne, som manglende eller utilstrækkelig informationssikkerhed kan medføre, der især påkalder sig opmærksomhed.

I forhold til personoplysninger kan to situationer sikkerhedsmæssigt forekomme. For det første kan den, der råder over oplysningerne (*den dataansvarlige*), selv opbevare dem og foretage dispositioner, og for det andet kan opbevaringen være overladt til nogen, der har bedre eller større teknisk kapacitet (*en databehandler*). Persondatalovens regler tager sigte på begge situationer, idet det først og fremmest er den dataansvarlige, der har ansvaret for, at sikkerheden er i orden.

Efter persondataloven skal den dataansvarlige "træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven". Det står også i loven, at personer, der arbejder for en dataansvarlig eller en databehandler, skal følge en instruks fra den dataansvarlige. Hvis den dataansvarlige benytter en databehandler, skal der være en skriftlig aftale mellem den dataansvarlige og databehandleren. Loven fortæller os således, at der skal være sikkerhed, og hvem der har ansvaret herfor, idet det også fremgår, at det er strafbart ikke at leve op til disse krav.

Loven fortæller os derimod ikke, hvilke mere præcise sikkerhedsforanstaltninger der skal være sat i værk, og ej heller om man skal bruge de samme foranstaltninger i alle situationer. Denne tavshed illustrerer en vigtig forskel på den juridiske og tekniske regulering af informationssikkerhed. Det er en almindelig iagttagelse, at de tekniske krav, der skal opfyldes for at opnå acceptabel sikkerhed, ofte er komplekse, og at de ikke er stationære, fordi de hele tiden må udvikles og tilpasses til nye former for teknologi. Kravene er i det hele taget betinget af, hvilken teknologi der bliver anvendt. Der er eksempelvis forskel på den situation, hvor personoplysninger opbevares i et centralt mainframe-system, og den situation, hvor oplysningerne er placeret i et netværk. Der er således mange forskellige momenter, som må tages i betragtning ved udformning af sikkerhedskrav. Det er endvidere karakteristisk, at mange sikkerhedskrav er teknisk formuleret, dels for at de kan være tilstrækkeligt præcise, og dels fordi de typisk skal realiseres af personer, der besidder teknisk sagkundskab.

Forhold af denne karakter fører til, at alle de forskellige detaljerede krav til sikkerhed, der skal opfyldes, ikke er et emne, som er egnet til at blive medtaget i en lov. For det første ville loven i så fald blive meget omfangsrig, og for det andet ville det være nødvendigt hele tiden at ændre loven, hvilket ikke er realistisk. En lov skal altid behandles flere gange af politikerne i Folketinget, og det tager ofte lang tid. Man må derfor bruge andre reguleringsformer, der bl.a. har den fordel, at de giver en vis fleksibilitet. Derfor har Folketinget bedt justitsministeren om at skrive de detaljerede regler, som skal bruges i de offentlige myndigheder. Justitsministeren kan hurtigt skrive reglerne om, hvis der fx kommer nye tekniske sikkerhedsløsninger eller nye behov. Folketinget har også bedt Datatilsynet om at hjælpe myndighederne med at overholde reglerne og om at holde øje med, om reglerne overholdes. Derfor har Datatilsynet skrevet en vejledning om reglerne om informationssikkerhed. Justitsministeren har ikke skrevet regler til de private virksomheder eller private organisationer om sikkerhed for personoplysningerne, hvilket ofte give anledning til en vis undren. Årsagen er formodentlig, at man ikke vil regulere den private sektor for tæt, samt at denne sektor er mere forskelligartet end den offentlige sektor. I praksis mener man dog, at private virksomheder som udgangspunkt skal følge de regler, der gælder for de offentlige myndigheder.

Hvordan skal en myndighed eller virksomhed opbevare data?

Ansvaret for at opbevare personoplysninger sikkert og forsvarligt ligger først og fremmest hos den myndighed eller virksomhed, der råder over oplysningerne (den dataansvarlige). Denne kan vælge selv at opbevare data og foretage dispositioner, eller opbevaringen kan overlades til nogen, der har bedre eller større teknisk kapacitet (en databehandler).

Der er ikke faste regler for, hvordan it-sikkerheden i en virksomhed eller myndighed skal gribes an i praksis. Det varierer – alt afhængigt af virksomhedens størrelse, hvor følsomme data der arbejdes med, og om der er adgang for eksterne til at logge sig på netværket. Helt overordnet skal der både internt og eksternt etableres det, som loven kalder "den fornødne sikkerhed".

De ansatte skal udvise en fornuftig adfærd

Arbejdsgivere skal fastlægge nogle rutiner eller indføre nogle systemer, som medfører, at de ansatte kun har adgang til de oplysninger, som de har ret til at anvende. Desuden skal arbejdsgiveren kontrollere, at de ansatte kun bruger personoplysningerne til de formål, som de må bruge dem til. De ansatte skal i det hele taget uddannes til at tænke på it-sikkerhed i deres omgang med computere og netværk. Dette kan typisk gøres ved kurser og interne kampagner, der fortæller om god it-adfærd.

> *En dataansvarlig skal som minimum sørge for, at der ikke ligger personoplysninger åbent tilgængelige på internettet*

Systemerne kan sikres på mange måder

Rent teknisk skal virksomheden sikre sig mod, at personer udefra kan trænge ind til personoplysningerne og herefter bruge, manipulere eller stjæle dem. Typiske foranstaltninger er firewalls og antivirusprogrammer. Internettet er en nyttig kilde til information, men også genstand for talrige målrettede forsøg på ulovlig indtrængen. En virksomhed eller myndighed skal som minimum sørge for, at der ikke ligger personoplysninger åbent tilgængelige på internettet, der kan opsnappes og bruges af andre.

Er alt dette vellykket, hvad det langtfra altid er, er der skabt en større sandsynlighed for, at borgerne opnår den databeskyttelse, som lovgivningen tilsigter.

Virksomheder og myndigheder har en stor interesse i at beskytte deres oplysninger, fordi de repræsenterer en betydelig værdi. Herudover bidrager de teknologiske sikkerhedsløsninger også til at forebygge kriminalitet og undgå andre sikkerhedstrusler som følge af fx hacking. Undertiden udtrykkes dette, som at "svaret på teknologien er teknologien".

Kravene til it-sikkerhed skal være realistiske

Kommet så langt er spørgsmålet, hvilke krav virksomheden eller myndigheden skal stille til sin informationssikkerhed. I første omgang er dette ikke et teknisk spørgsmål, men snarere et samfundsmæssigt. Spørgsmålet opstår først og fremmest, fordi sikkerhed ikke er gratis. Der må tages stilling til, hvor store ressourcer der skal anvendes til dette formål. Spørgsmålet kan også vendes om: Hvilken pris skal virksomheden eller myndigheden betale for adgangen til at behandle personoplysninger?

Når dette spørgsmål er relevant, skyldes det, at personoplysninger er informationssamfundets primære grundstof, og at der derfor er en almindelig samfundsmæssig interesse i, at der er adgang til at benytte disse oplysninger. Nogle sikkerhedskrav er som udgangspunkt uønskelige, hvis de er så omkostningskrævende, at de reelt hindrer myndigheder eller virksomheder i at benytte personoplysninger på en teknologisk fornuftig måde. Kravene må fastlægges under hensyntagen til de generelle samfundsmæssige behov.

Denne indfaldsvinkel fører til, at sikkerhedskravene skal være realistiske. De kan også være forskellige, alt efter hvilke personoplysninger der anvendes, og måden, det sker på. Kravet er, at der skal være en *tilstrækkelig* sikkerhed. Det er altså ikke et krav, at der skal anvendes den nyeste eller absolut bedste sikkerhedsløsning (state of the art). Herudover afhænger sikkerhedsniveauet af andre forhold. Man kan eksempelvis se på, om der behandles følsomme eller almindelige personoplysninger, om formålet med behandlingen kan være risikabelt for personernes integritet, og om oplysningerne befinder sig i eller transmitteres i netværk. Alt i alt skal sikkerheden ikke være optimal, men den skal være *tilstrækkelig* til, at der foreligger en reel databeskyttelse.

Skal sikkerhedskravene forstås af alle – eller bare virke?

Sikkerhedsforanstaltninger kan være komplekse eller simple, idet begge typer kan give anledning til vanskeligheder. Der kan være tale om løsninger, hvis anvendelse enhver kan forstå, og løsninger, der alene kan gennemskues af personer, som har høj teknologisk indsigt. Nogle løsninger er lette at anvende, mens andre er eller opleves som besværlige (mere om dette under 5).

Som udgangspunkt er det ikke et krav, at sikkerhedsforanstaltningen skal kunne forstås af enhver. Den skal blot virke og kunne leve op til sit formål. I færdselslovgivningen stilles der tilsvarende en række krav til biler, og de skal – og bliver det for det meste – overholdes, uden at det er et krav, at den enkelte bilist forstår, hvordan de virker. Afgørende er funktionen. Det gælder også i forhold til informationsteknologien.

Megen informationsteknologi er svær at forstå

Foranstaltningen skal gøre teknologien sikker, således at personoplysningerne befinder sig i et trygt miljø. Selvom reglerne ikke kræver, at de, som anvender personoplysninger, har teknologisk viden, kræver de, dels at der er sikkerhedsløsninger til rådighed, og dels at de anvendes i passende omfang. Begge dele forudsætter, at der er en vis forståelse af de risici, som brugen af teknologien repræsenterer. Denne forudsætning er ikke altid opfyldt, fordi megen informationsteknologi er svær at forstå. Der er mange eksempler på, at truslerne ikke tages alvorligt. Nogle gange ser man også eksempler på, at sikkerhedsforanstaltningerne overdrives, fordi leverandørerne har en økonomisk interesse i at sælge sikkerhedsløsningerne.

Nogle illustrerende eksempler på sikkerhedsforanstaltninger

Den vel nok mest kendte sikkerhedsforanstaltning er *passwordet*. Den person, der er berettiget til at anvende en bestemt computer til bestemte formål, skal anvende en personlig kode for at kunne bruge computeren. Uanset at dette er en særdeles simpel foranstaltning, der tilsigter at holde andre ude, er den central i forhold til informationssikkerheden, fordi den giver mulighed for at identificere brugeren og om fornødent registrere (logge) anvendelsen af personoplysninger. Så er der større sandsynlighed for, at misbrug opdages. Alt dette er dog ikke ensbetydende med, at brugen af passwords er en selvfølge, eller at de anvendes på en forsvarlig måde. Det er nødvendigt at huske passwordet, hvilket gør brugen af personoplysninger mere besværlig.

I en af de mest kendte sager, som Datatilsynet har haft i nyere tid, måtte tilsynet anvende et års tid på at få politiet til at anvende passwords på de enkelte stationer, hvor computerne hidtil havde stået åbne, således at enhver i lokalet frit kunne anvende dem. I forhold til en dataansvarlig, der behandler meget private personoplysninger, gav selv en simpel sikkerhedsforanstaltning anledning til vanskeligheder. Reglerne om sikkerhed er klare og lette at forstå, men det er ikke ensbetydende med, at praksis er i overensstemmelse hermed. Passwords skal behandles fortroligt, men der er sikkert fortsat en del tilfælde, hvor de er skrevet på en lap papir ved siden af computeren


Backspa
Enter
Shift
Ctrl

eller på tilsvarende måde ikke holdt fortrolige. Den menneskelige faktor vil altid udgøre et svagt led i sikkerheden.

Der spørges ofte om, hvorvidt sikkerhedsfejl kan afdækkes. Svaret herpå er, at det kan de ikke fuldt ud, men Datatilsynet råder over visse muligheder for at opdage dem. Myndigheder og virksomheder, som registrerer og behandler persondata, skal altid give Datatilsynet besked, når de registrerer og bruger personoplysninger. Det sker ved, at den dataansvarlige myndighed eller virksomhed sender en anmeldelse til Datatilsynet, hvor de beskriver de personoplysninger, de registrerer, og hvad de bruger dem til. Datatilsynet kan så gennemføre inspektioner hos de offentlige myndigheder og private virksomheder og organisationer, som registrerer og bruger personoplysninger. Disse inspektioner kræver mange ressourcer og gennemføres derfor kun i begrænset omfang. De har ikke alene til formål at gennemføre kontrol, men danner ligeledes rammen om en dialog mellem virksomheden eller myndigheden og Datatilsynet. Her kan man bl.a. drøfte, hvorledes sikkerheden bedst tilrettelægges i den konkrete myndighed eller virksomhed. Når det er muligt, kan man finde frem til pragmatiske løsninger.

Et andet spørgsmål er, hvilket sikkerhedsniveau man overhovedet kan kræve. Dette afhænger af den risiko, som brugen af en bestemt teknologi i forhold til bestemte typer af personoplysninger indebærer. Svaret på spørgsmålet kræver indsigt i både jura og teknik.

Et klassisk spørgsmål drejer sig om, hvordan man bedst beskytter e-post. Set med juridiske øjne er en e-post et brev (”lukket meddelelse”). Læser andre personer en e-post uden tilladelse, sker der et brud på brevhemmeligheden. Spørgsmålet er nu, om en e-post faktisk svarer til et brev, eller om den snarere kan sammenlignes med et åbent postkort. Ved udformningen af kravene i lovgivningen har man sidestillet e-post med et åbent postkort. Det har haft den konsekvens, at fortrolige eller følsomme personoplysninger ikke kan sendes med e-post, medmindre de er beskyttet. Hovedmidlet har været *kryptering*, der netop værner kommunikationsindholdet, men ikke de kommunikerendes identitet. Som det vil fremgå nedenfor, giver kryptering dog også

Krypteringsproblemet belyst ved et eksempel

Problemstillingen har været aktuel i forbindelse med en sag om reservationer over internettet af bøger fra biblioteker. Når der reserveres bøger ved brug af e-post, resulterer det i en tilsvarende kvittering pr. e-post fra biblioteksdatabasen. Da det er fortroligt, hvilke bøger en borger låner på biblioteker, skal denne kvittering krypteres, hvilket i praksis betyder, at et sådant system ikke fungerer.

Den aktuelle sag endte med, at biblioteksvæsenet fik en dispensation, der oprindelig var tidsbegrænset, men i foråret 2010 blev forlænget indtil videre. Dispensationens baggrund er, at borgeren efter Datatilsynets opfattelse ikke skal kunne give samtykke til at modtage ukrypteret post. Dette vil svare til at kræve et samtykke til en reduceret sikkerhed. Når det tages i betragtning, hvor ressourcekrævende sikkerhed og kryptering er, ville ordningen formentlig resultere i, at mange flere dataansvarlige ville forsøge at opnå et sådant samtykke, hvorved databeskyttelsen på denne måde blev undergravet. Sagen har udløst stor debat og illustrerer et væsentligt problem i forbindelse med sikkerhed.

anledning til problemer. Selvom krypteringskravet fortsat opretholdes i vidt omfang, er holdningen blevet en anelse mere afslappet. Det skyldes måske manglende kendskab til teknologien, når e-posten uden forbehold sammenlignes med postkortet. Det kræver således en vis teknologisk viden at skaffe sig adgang til andres e-post. Den er vel ikke sikret, men den er heller ikke åben for enhver.

Selvom kryptering i og for sig er en enkel løsning, er denne metode ikke problemfri, fordi det ikke er alle, der er i stand til at læse en krypteret e-post. Faktisk er det de færreste, der er i stand til det. Det har derfor været diskuteret, om en person skulle gives adgang til at sige ja til at modtage ikke-krypteret e-post, selvom den indeholder følsomme eller fortrolige oplysninger.

Sikkerhedsløsninger skal være brugervenlige

Udgangspunktet for reglerne i persondataloven er, at den moderne informationsteknologi er nyttig, og at det er vigtigt for samfundet, at den anvendes. Men det skal ske på en civiliseret måde. Teknologien skal kunne anvendes efter hensigten – og det er samtidig ikke meningen, at sikkerhedsløsningerne skal forhindre anvendelsen. Derfor bør sikkerhedsløsningerne være brugervenlige. Brugen af personoplysninger er så udbredt – også i privatsfæren – at det i mange tilfælde er den enkelte person, der selv må beskytte sine oplysninger. Ikke mindst på internettet er personen ofte alene. Som det omtales nærmere nedenfor, burde sikkerheden ideelt fungere helt uafhængigt af brugeren, men dette er langtfra altid tilfældet.

> ***Sikkerheds-løsningerne skal ikke forhindre anvendelsen***

Et velkendt eksempel på de problemer, som manglende brugervenlighed kan medføre, er anvendelsen af den *digitale signatur.* Denne beskyttelsesforanstaltning bruges til at dokumentere, hvem brugeren er, hvilket er nødvendigt i den virtuelle verden, hvor vi ikke mødes fysisk, fx i kontakten mellem borger og myndighed via selvbetjeningsfunktionen på en hjemmeside. Signaturen har dog vist sig alt for svær at anvende. Det er en udbredt erfaring, at en internettjeneste ikke bruges i det tilsigtede omfang, hvis det er en betingelse, at der skal benyttes digital signatur. Dette er naturligvis ikke hensigtsmæssigt, og det er derfor en væsentlig ambition bag reglerne om informationssikkerhed, at det tilstrækkelige sikkerhedsniveau ikke blot er til stede, men samtidig har den fornødne brugervenlighed. Som allerede nævnt er dette ikke nogen nem målsætning at realisere.

Virksomheder og myndigheder skal forberede sig på sikkerhedstruslerne

Sikkerhed kommer som bekendt ikke af sig selv. Det er vanskeligt for en del dataansvarlige at vælge den teknologi, som bedst sikrer persondatabeskyttelsen i netop deres virksomhed eller myndighed. Det tager tid, og det kan være fristende at lade være med at afsætte de nødvendige ressourcer. For at modvirke dette fænomen er det en fremtrædende tendens i lovgivningen, at der stilles mere systematiske krav til den dataansvarlige.

Er der eksempelvis tale om et større informationsteknologisk system som fx et komplekst økonomistyringssystem med fortrolige data, mange forskellige brugerroller eller flere separate registre, der ikke må samkøres, stiller Datatilsynet i dag ofte krav om, at der i forvejen skal være gennemført en analyse af de konsekvenser for databeskyttelsen, som det pågældende system har. Infrastrukturen skal være kortlagt, og der skal være foretaget en såkaldt PIA (privacy impact assessment, bedst oversat som vurdering af konsekvenser for persondatabeskyttelsen), hvori sikkerhed indgår som et vigtigt forhold. Virksomheden eller myndigheden skal således være på forkant med de udfordringer, som en bestemt anvendelse af personoplysninger har, således at det på forhånd kan udelukkes, at misbrug af personoplysninger vil forekomme.

Når det gælder selve udformningen af teknologien, er det også karakteristisk, at der ikke findes regler for teknologien som sådan, fordi teknologien hele tiden udvikler sig, og man kan derfor kun vælge den teknologi, som lever op til de gældende sikkerhedskrav.

En lovmæssig regulering indebærer en risiko for, at kravene alligevel ikke opfyldes, fordi det ikke er sikkert, at den dataansvarlige kan administrere de frihedsgrader, der er fastlagt. På denne baggrund er der nu introduceret et nyt begreb, *privacy by design*, som betyder, at den nødvendige sikkerhed skal være indbygget i den teknologiske løsning på forhånd.

Et eksempel kan være, at persondata krypteres og dekrypteres, uden at brugeren selv behøver at gøre noget for, at dette sker. Den teknologi, der benyttes til at behandle personoplysninger, skal generelt være beskyttende (*privacy enhancing technology*), bl.a. ved at tilvejebringe en god sikkerhed. Dette betyder ikke nødvendigvis, at teknologien er brugervenlig, selvom dette også er en forventning. Det øger dog sandsynligheden for, at der ikke sker misbrug af personoplysningerne.

Privacy by design, der ikke i skrivende stund er indarbejdet i persondataloven, behøver ikke i sig selv at få en positiv betydning. Det jo ikke er sikkert, at den dataansvarlige faktisk benytter disse former for teknologi. Der skal derfor endnu mere til. Dette "mere" kunne være, at der gennemføres en certificeringsordning for den teknologi, der må benyttes til at behandle persondata, i hvert fald i større sammenhænge. Med en certificeringsordning vil en bestemt teknologi være udpeget til at være privatlivsbeskyttende. Denne teknologi, der kan være en blandt flere anvendelige muligheder, vil kunne benyttes af den dataansvarlige i forhold til bestemte former for behandling af personoplysninger. Det er på mange måder et ambitiøst og krævende projekt, der er udtryk for den opfattelse, at sikkerhedsniveauet i dag (2010) generelt bedømt ikke er tilfredsstillende.

Vedtages der en certificeringsordning, bliver det en blandet juridisk og teknisk opgave at foretage de vurderinger, der er nødvendige for valget af egnede teknologier. Som udgangspunkt fastlægger juristerne de krav, der skal opfyldes, hvorefter det teknisk kan vurderes, om en bestemt teknologi lever op til disse krav. Der er således tale om en tværfaglig opgave, hvor det er væsentligt, at jurister og teknisk kyndige forstår hinanden. Denne opgave er særlig krævende, fordi personoplysninger anvendes internationalt. Skal en certificering have nogen mening, må den i princippet gælde overalt. Den konstante transmission af personoplysninger via internettet illustrerer, at rent nationale løsninger har begrænset værdi og endda skader konkurrenceevnen for de dataansvarlige, som forpligtes af dem. Det er derfor sandsynligt, at hvis denne ordning gennemføres, bliver der i det mindste tale om en form for EU-certificering.

Sikkerhedsbrister opdages ofte rent tilfældigt

I disse år er der en fornyet fokus på behovet for sikkerhed. I vidt omfang er det en tværfaglig opgave at realisere den sikkerhed, der er påkrævet for at sikre personoplysninger imod misbrug. Uanset de mange bestræbelser er det dog ikke realistisk at forestille sig, at der aldrig sker sikkerhedsbrud. Spørgsmålet er, dels hvordan man bliver klar over, at der er sket et sådant brud, dels hvilke konsekvenser det har.

Nogle sikkerhedsbrud afdækkes nærmest af sig selv, fordi de har så store konsekvenser, at de uden videre opdages, eksempelvis tyveri af pc'er med fortrolige data eller hacking, der medfører

Gode råd om it-sikkerhed

IT- og Telestyrelsens hjemmeside giver med domænet it-borger.dk/sikkerhed et glimrende overblik over junglen af it-sikkerhedstrusler samt midler til at imødegå dem. Eksemplerne nedenfor på typiske sikkerhedstrusler anno 2010 er således hentet fra denne side, som også giver en udtømmende oversigt over tekniske og adfærdsmæssige forholdsregler.

SPYWARE

Spyware er små spionprogrammer, som – uden din viden – indsamler informationer om dine interesser og vaner på internettet. Disse informationer sender spywaren tilbage til bagmændene, som enten selv bruger oplysningerne i reklameøjemed eller sælger oplysningerne videre til andre.

Cookies
Cookies anvendes til at gemme oplysninger om dig på din egen computer. Cookies er som regel ikke skjult for brugerne, men du kan forhindre, at der gemmes cookies på din computer ved at ændre i din browsers internetindstillinger under fanebladet sikkerhed.

Adware
Adware-programmer er mere harmløse end spyware, da de ikke sender information tilbage til bagmændene uden din viden. Adware kan vise pop op-vinduer med reklamer, ændre dine indstillinger i browseren (for eksempel startsiden), installere uønskede søgemenuer eller tilføje bookmarks i browseren.

Browserhijack
Browserhijacking (kidnapning af din browser) forveksles tit med spyware. Browserhijacking er, hvis du bliver ført til en anden hjemmeside end forventet, selvom du har indtastet den korrekte webadresse.

Keyloggere
En keylogger er en form for spyware, som er et lille program, som registrerer, hvilke taster du trykker på, og herefter sender det til bagmanden. Dette kan for eksempel bruges til at opfange passwords eller anden fortrolig information.

Malware
Malware er en sammenskrivning af "malicious software", som betyder ondsindede programmer. Malware er betegnelsen for ethvert program, som er ondsindet over for en bruger. Malware dækker både over vira, orme, trojanske heste, keyloggere, spyware og lignende.

VIRUS

En computervirus er et program, der er i stand til at sprede sig til andre computere. Virussen kan ligge i et program eller en fil og udføre skadelige aktiviteter på din computer, fx slette filer eller programmer.

Orm
En orm er ikke knyttet til et program eller en fil. Ormen spreder sig selv over det netværk, som computeren er tilkoblet. Det kan både være det lokale netværk eller internettet. Da ormen er afhængig af en forbindelse over et netværk, er servere de mest udsatte, fordi de som regel har fast forbindelse til nettet.

Trojansk hest/bagdør
En trojansk hest er et program, der giver en "hemmelig" adgang til din computer. Den trojanske hest kan fx være skjult i et spil eller program, du har downloadet fra en hjemmeside, eller din computer kan være inficeret af en virus, der selv har installeret den trojanske hest. Hackere eller virusbagmændene kan bruge den trojanske hest til at få adgang til din computer, og dermed får de mulighed for at overtage kontrollen med din computer, herunder finde fortrolige oplysninger, gemme ulovlige programmer eller bruge din computer til at sende spam til andre.

Hoax
Hoax betyder spøg eller svindelnummer. En hoax er altså ikke en egentlig virus eller et program, men en falsk advarsel i en e-mail om en virus, der ikke findes. En hoax spredes ved, at folk i god tro sender advarslen videre. En hoax kan fx have en tekst, hvor der står noget i retning af: "Send straks denne advarsel videre til alle dine venner".

PHISHING – IDENTITETSTYVERI

Identitetstyveri sker, når personer tilegner sig andres personoplysninger og udgiver sig for at være disse personer. Det kan ske elektronisk ved brug af bankoplysninger, CPR-numre eller kodeord eller ved at bruge den andens id-papirer (sygesikringsbevis, kørekort m.m.). Der er også tale om identitetstyveri, når en person køber produkter, fx over internettet, ved hjælp af en andens person- og kontooplysninger. Phishing foregår, hvis man modtager en falsk e-mail, der ser ud til at komme fra en bank, onlinebutik, forsikringsselskab eller en anden troværdig afsender. I e-mailen opfordres man til at opgive personoplysninger, numre på betalings- og kreditkort, kontonumre, CPR-numre, pinkoder eller lignende og derpå sende e-mailen tilbage med oplysningerne.

MOBILSVINDEL VIA "ONE-RING FRAUD"

Som mobilbruger får du ofte en sms om, at en person forgæves har forsøgt at få kontakt med dig. Men ringer du op på det nummer, der bliver vist, kan du i særlige tilfælde komme til at betale dyrt.

FUPHJEMMESIDER

Staver du forkert, når du taster en netadresse ind i din browser, kan du risikere at havne på en hjemmeside, der indeholder skadelige programmer. Skriver du fx www.qZl.dk i stedet for www.qXl.dk eller www.kraRk.dk i stedet for www.krak.dk, kan du lande på en hjemmeside, der er designet til svindel.

Kilde: www.it-borger.dk/sikkerhed

systemnedbrud eller afsætter klare visuelle aftryk. I andre tilfælde er det mindre klart, om en uhensigtsmæssig anvendelse af personoplysninger skyldes et sikkerhedsbrud, og ligeledes uklart, hvor og hvornår dette er sket. Det kan være, hvis personer i en virksomhed eller myndighed bevidst eller ubevidst udnytter deres adgang til persondata på en uhensigtsmæssig eller uautoriseret måde. Datatilsynet har begrænsede ressourcer, og uanset adgangen til at foretage inspektioner er det ikke sandsynligt, at tilsynet bliver opmærksomt på alle de sikkerhedsbrud, der rent faktisk forekommer. Det er ligeledes usandsynligt, at borgerne altid opdager disse brud.

På denne baggrund er der indført et nyt middel, der i første omgang kun gælder for elektroniske kommunikationstjenester, men som forventes at komme til at gælde generelt, nemlig en meddelelsespligt. Den dataansvarlige har således nu pligt til at orientere Datatilsynet om sikkerhedsbrud, der har haft en praktisk betydning. Hvis sikkerhedsbruddene også indebærer en risiko for integritetskrænkelser, skal de berørte borgere informeres. Denne meddelelsespligt ("*breach notification*") skal bl.a. skabe større åbenhed om sikkerhedsniveauet. Det forudsætter dog, at den dataansvarlige faktisk giver denne meddelelse. Selvom dette næppe vil ske i alle tilfælde, er det sandsynligt, at de myndigheder og virksomheder, der er ansvarlige for mange personoplysninger, vil respektere denne ordning, som dermed sandsynligvis vil bidrage til at skabe en bedre sikkerhed og dermed større tryghed.

Når det konstateres, at der er sket et sikkerhedsbrud, kan retssystemet, dvs. politiet og domstolene, reagere på forskellige måder. Den dataansvarlige kan blive straffet for at overtræde sikkerhedsreglerne, men det er ganske sjældent, at nogen bliver straffet for sikkerhedsbrud. I princippet kan den krænkede person kræve erstatning, hvis den dataansvarlige kunne have gjort noget for at undgå, at den registrerede led et økonomisk tab. Men sådanne erstatningskrav fremsættes stort set aldrig. Det er kun i forhold til få typer af persondatabehandling, at et sikkerhedsbrud kan få den konsekvens, at den dataansvarlige fratages retten til at behandle persondata. Det ville forudsætte, at der gentagne gange er forekommet store sikkerhedsbrud. Reglen er endnu aldrig blevet brugt, og det er som nævnt også sjældent, at der sker andre reaktioner. I forhold til reaktionsmidler kan man godt konkludere, at retssystemets præstation ikke er imponerende.

Datasikkerhed – den endeløse saga

Den gode sikkerhed opstår nok først og fremmest, fordi det er i den dataansvarliges egen interesse at fremme den, eller fordi den dårlige omtale, som sikkerhedsbrud kan føre til, er både økonomisk og image-mæssigt skadelig for den dataansvarliges virksomhed. Selvom der hele tiden vedtages nye regler, der tager sigte på at fremme god informationssikkerhed, og selvom der samfundsmæssigt er stor fokus på dette område, vil emnet også fremover være højt profileret.

Der har altid været og vil fremover blive ved med at være god og dårlig sikkerhed. Der vil også fremover være en kamp mellem de teknologier, der understøtter databeskyttelse, og teknologier, der undergraver denne beskyttelse. Denne kamp slutter næppe nogensinde, og den er særlig fremtrædende i disse år, hvor nye teknologier og nye måder at anvende kendt teknologi på konstant viser sig. Teknologien og juraen må stå side om side i denne kamp. Målet og håbet må være, at de fleste sejre vindes af de teknologier, der skaber den gode sikkerhed og dermed den effektive beskyttelse af borgernes personlige integritet og privathed. ❖

Læs mere

Peter Blume: *Databeskyttelsesret* (3.udg. 2008 DJØF Forlag)
Peter Blume, Janne Rothmar Herrmann: *Ret, privatliv og teknologi* (2.udg. 2010 DJØF Forlag)

PETER BLUME

Peter Blume har siden 1993 været professor i retsinformatik på Det Juridiske Fakultet på Københavns Universitet. Peter Blume blev cand.jur. i 1974, lic.jur. i 1982 og dr.jur. 1989 og var institutleder på Retsvidenskabeligt Institut i perioden 1982-2002. Han er og har været medlem af adskillige råd og udvalg, herunder Datarådet, Akademisk Råd, Registerlovsudvalget samt formand for TV-overvågningsudvalget i 2006.

I dag er Peter Blumes primære forskningsområde persondataret samt juridisk metode, som han også underviser i på Københavns Universitet. Af udvalgte publikationer kan nævnes: "Databeskyttelsesret (2008)" og "Persondataretten – nu og i fremtiden" (2010).

Den digitale revolution – fortællinger fra datalogiens verden
Bogen er udgivet af Datalogisk Institut, Københavns Universitet (DIKU) i anledning af instituttets 40 års jubilæum med bidrag fra forskere tilknyttet instituttet.

Redaktion:
Tariq Andersen, phd-studerende, Jørgen Bansler, professor, Hasse Clausen, lektor,
Inge Hviid Jensen, kommunikationsmedarbejder og Martin Zachariasen, institutleder.
Forsidemotiv: Foto af skulptur af Alan Turing, © basegreen lokaliseret på flickr.om/photos/basegreen
Oplag: 1000 eks.
Grafisk design og produktion: Westring + Welling A/S
ISBN: 978-87-981270-5-5