
Sikkerhed for børn i online sociale tjenester

1	Sammenfatning af analysen.....	2
2	Formål	2
3	Afgrænsning	3
4	Målgruppe	3
5	Misbrugssituationer.....	3
5.1	Krænkelser.....	4
5.2	Overgreb.....	5
5.3	Karakteristika ved misbrugssituationer.....	5
6	Mulige tiltag.....	6
6.1	Oplysning	6
6.2	Tekniske tiltag.....	7
6.3	Regelbaserede tiltag	10
7	Anbefalinger	10
7.1	Oplysning	10
7.2	Tekniske tiltag.....	11
7.3	Regelbaserede tiltag	12
	Bilag 1: Referenceliste	13

IT- og Telestyrelsen

Holsteinsgade 63

2100 København Ø

Telefon 3545 0000

Telefax 3545 0010

E-post itst@itst.dk

Netsted www.itst.dk

CVR-nr. 26769388

Side 1/14

1 Sammenfatning af analysen

Videnskabsminister Helge Sander var i åbent samråd i Videnskabsudvalget den 11. juni 2008 vedrørende en såkaldt digital ungdomssignatur¹. Som opfølgning herpå har IT- og Telestyrelsen udarbejdet denne analyse af de eksisterende muligheder for beskyttelse af børn på online sociale tjenester på internettet.

Analysen omfatter en afklaring af misbruget af børn og unge ved anvendelse af online sociale tjenester samt af muligheder for yderligere at styrke oplysningsindsatsen og tekniske tiltag på området. Udgangspunktet for analysen er fem spørgsmål, der blev formuleret af ministeren på samrådet:

1. Hvad slags løsning er i det hele taget bedst og mest sikker?
2. Kan indførelse af en digital signatur for børn og unge overhovedet løse problemet, eller skabes der bare falsk tryghed og sikkerhed?
3. Hvad skal aldersgrænsen for en ungdomssignatur være?
4. Vil de unge overhovedet bruge signaturen?
5. Vil tjenesteudbydere af chatfora bruge mulighederne?

IT- og Telestyrelsen

Side 2/14

Analysen viser, at situationen omkring misbrug af børn som følge af dialog initieret på online sociale tjenester er kompleks. En teknisk løsning kan ikke egenhændigt beskytte børn og unge. Tiltag til beskyttelse af børn på online sociale tjenester bør bringe flere virkemidler i anvendelse. Børnene bør have størst mulig valgfrihed og navigationsrum samtidig med, at de selv og deres ret til privatliv beskyttes.

Tiltag bør fremme de nuværende oplysningstiltag samt kigge nærmere på mulighederne for teknisk at integrere autentifikation, for eksempel af alder, i online sociale tjenester. Tiltag bør forankres i et frivilligt organ, der ved koordination og konsensuskabelse kan sikre handling på området.

2 Formål

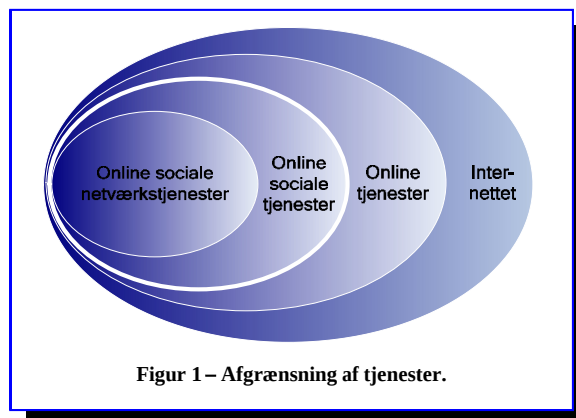
Analysen skal:

- afdække omfanget af samt karakteristika ved misbrugssituationer, der involverer børn, og som er en direkte følgevirkning af brugen af online sociale tjenester
- inddrage overvejelser om hensynet til privatlivets fred ved brug af online sociale tjenester og
- identificere elementer, der kan indgå i beskyttelsestiltag, som kan imødegå misbrugssituationer.

¹ UVT – almindelig del – spørgsmål R.

3 Afgrænsning

Tjenester på internettet kan inddeles i forskellige kategorier. Online tjenester omfatter mange former for services fra e-handel over tjenesterne på borger.dk til netbanker. Ens for alle disse tilbud er, at modtageren – borgeren – har mulighed for at benytte en facilitet som hjemmesiden stiller til rådighed. En delmængde af disse tjenester kan kategoriseres som online sociale tjenester, det vil sige tjenester, hvor brugeren kan indgå i dialoglignende kontakt med andre brugere. Hjemmesiden kan for eksempel indeholde interaktion såsom chat, e-mail eller andre former for beskeder mellem brugerne.



IT- og Telestyrelsen

Side 3/14

Endelig er online sociale netværkstjenester en delmængde af disse online sociale tjenester, da disse netværkstjenester ud over interaktionselementet også indeholder en netværksdel, der gør det muligt for brugeren at oprette og se egne og andres lister over venner. Figur 1 illustrerer sammenhængen mellem de forskellige typer af tjenester på internettet.

Analysen omfatter de områder, hvor børn kommer i dialoglignende kontakt med andre, det vil sige online sociale tjenester, herunder online sociale netværkstjenester. Analysen omfatter ikke tjenester, der henvender sig specifikt til voksne, eksempelvis netbanker og dating sites, eller hvor hovedformålet for tjenesten ikke er det sociale element. Analysen afgrænses desuden til kun at omfatte relationen voksen-barn.

4 Målgruppe

Analysens målgruppe er børn under 15 år. Dette er den seksuelle lavalder og dermed grænsen for, hvornår børn kan forventes at tage vare på sig selv i forhold til indgåelse af seksuelle relationer.

5 Misbrugssituationer

Undersøgelser viser, at langt de fleste børn bruger online tjenesterne til at kommunikere med de venner, de har i den fysiske verden. Det er desuden påvist, at flertallet af børn, der benytter online sociale tjenester anonymt, gør det for at forhøre sig om andres erfaringer med hensyn til kærlighed og sex og til at forsøge sig med forskellige identiteter. Størstedelen af børn bliver ikke udsat for misbrug i forbindelse med deres brug af internettet.

Udsatte børn er børn med dårlig social og kulturel integration og/eller børn med personlighedsmæssig dysfunktion.

Medierådet 2008

De børn, der bliver udsat for ubehagelige oplevelser, falder ifølge nationale og internationale undersøgelser² typisk ind under kategorien for udsatte børn. Hertil kommer en lille gruppe af velfungerende børn, som i pubertet og præpubertet eksperimenterer med deres seksuelle fantasier.

Med hensyn til en misbrugssituation kan der skelnes mellem to typer af misbrug: Krænkelser og overgreb. De følgende underafsnit omhandler karakteristika ved disse to typer af misbrugssituation.

5.1 Krænkelser

Krænkelser er det problem, der oftest forekommer i kontakten mellem barn og voksen på online sociale tjenester.

Kontakten ved krænkelser mellem voksen og barn sker typisk på to forskellige måder:

En krænkelser er en handling, som overtræder barnets grænser og gør det uroligt, ked af det eller bange.

IT- og Telestyrelsen

Side 4/14

1. *Den direkte metode:* Den voksne er åbenlys og hurtig i sine kontakter med børnene og lægger ikke skjul på sine hensigter. De børn, som reagerer på denne type henvendelser, er som regel nysgerrige, ressourcestærke børn, som også siger fra, når den voksne bliver for nærgående.
2. *Den indirekte metode:* Den voksne går langsomt og forsigtigt til værks og groomer barnet, det vil sige opbygger en tillids- og fortrolighedszone i forhold til barnet, så barnet føler, at her har det fået en voksen-ven. Den unikke opmærksomhed og interesse gør, at barnet honorerer den voksne med et loyalt venskab. Børnene beskriver, at de godt ved, at man ikke skal udlevere private oplysninger. Men de betragter den voksne som en personlig og nær ven. En ven, som det også er naturligt at blive ven med i den virkelige verden. Ydermere tager den voksne typisk kontakten over på et medie, der ikke overvåges, når tilliden hos barnet er vundet, for eksempel chat klienter som Microsoft Messenger eller ICQ.

Undersøgelserne viser endvidere, at³

- 4,5 procent af de adspurgte børn har været udsat for uønskede, anstødelige henvendelser,
- 1,5 procent har været udsat for foruroligende, seksuelle henvendelser og

² Alle faktuelle tal og statistikker i afsnittet og følgende underafsnit baserer sig på uddrag af danske og udenlandske undersøgelser, disse er refereret i fodnoter hvor relevant. Endvidere indeholder bilag 1 en samlet liste af referencer.

³ Kilde: Youth Internet Survey (2006), Crimes against Children Research Center, University of New Hampshire

- 1,9 procent har været udsat for pågående seksuelle henvendelser, herunder opfordring til offline kontakt.

Kun fem procent af de voksne lyver om deres alder og udgiver sig for at være mindreårige. 79 procent af de voksne er ærlige om deres seksuelle ønsker i relation til den mindreårige.

Youth Internet Survey 2005

5.2 Overgreb

Overgreb omfatter de alvorligste handlinger, som dog sker sjældent. En opgørelse fra Rigshospitalets team for seksuelt misbrugte børn anfører, at der i perioden 2001-2007 var ti af teamets sager, der var startet med grooming via internettet.

En amerikansk undersøgelse⁴ har set på mønstre blandt de børn, der i løbet af et år **har oplevet** seksuelt orienterede henvendelser:

- 74 procent af henvendelserne resulterer i møder i det virkelige liv,
- 68 procent medfører ulovlig seksuel kontakt mellem barn og voksen⁵, herunder både frivillig og ufrivillig kontakt og
- 54 procent af børnene møder den voksne mere end én gang⁶.

Et overgreb kan defineres som en handling, som er strafbar i henhold til straffeloven:

- *Systematisk optagelse af utugtige billeder § 230*
- *Blufærdighedskrænkelser § 232*
- *Anden kønslig omgængelse end samleje § 224*
- *Voldtægt § 222*

Medierådet 2008

IT- og Telestyrelsen

Side 5/14

5.3 Karakteristika ved misbrugssituationer

Misbrugssituationer, både i form af krænkelser og overgreb, involverer typisk særligt udsatte børn, og har følgende karakteristika:

1. *Mindre end to børn pr. år* udsættes i gennemsnit for overgreb som følge af internet-initieret kontakt i Danmark.
2. *Kontakt mellem voksen og barn foregår som et venskab*. Den voksne opbygger gennem tillid og fortrolighed et venskab med barnet.
3. *De voksne lyver kun sjældent om deres alder eller seksuelle hensigter*. Kun fem procent af voksne brugere lyver om deres alder overfor barnet. 79

⁴ Janis Wolak et al (2004) – "Internet-initiated Sex Crimes against Minors: Implications for Prevention Based on Findings from a National Study". Journal of Adolescent Health 2004, vol. 35. Undersøgelsen omhandler alene mønstre blandt ofre for grove krænkelser og bygger på data fra føromtalt Youth Internet Survey (1999).

⁵ Undersøgelsen viser, at i 93 procent af de aftalte møder, der bliver til noget, er der på et tidspunkt tale om seksuel kontakt. Det vil sige i alt 68 procent af de børn, der er ofre for seksuelle krænkelser med opfordring til offline kontakt udsættes for seksuel kontakt.

⁶ Undersøgelsen opgør, at 73 procent af de 74 procent der mødes med den voksne offline, gør det mere end én gang. Det vil sige totalt set 54 procent af de børn, der er ofre for seksuelle krænkelser med opfordring til offline kontakt, mødes med den voksne mere end én gang.

procent er ærlige omkring seksuelle ønsker i relation til barnet efter at kontakten er etableret.

4. *Dialogen, ud over den indledende, flyttes over på en ikke-overvåget platform.* Så snart venskabet er etableret, flyttes kommunikationen mellem parterne over på ikke-overvågede tjenester som Microsoft Messenger eller på SMS via mobiltelefonen.

6 Mulige tiltag

Som det fremgår af karakteristika ved misbrugssituationer, er der tale om meget få overgreb på børn årligt i Danmark. Overgrebene sker ved hjælp af komplekse mekanismer baseret på at vinde barnets tillid og på at anvende ikke-overvågede tjenester. Det er mekanismer, der gør det svært at adresse hele problemstillingen med et enkelt tiltag.

Beskyttelse af børn og unge på online sociale tjenester kan ikke etableres *alene* ved hjælp af tekniske foranstaltninger.

IT- og Telestyrelsen

Tekniske foranstaltninger er et blandt flere tiltag, der kan gøres for at beskytte børn og unge på online sociale tjenester. For eksempel hjælper tvungen identifikation på online sociale netværkstjenester ikke, hvis den voksne i forvejen ikke lyver om, hvem han er. Eneste konsekvens bliver da, at barnets identitet med sikkerhed afsløres overfor den voksne. For at imødegå den komplekse problemstilling må tiltag ske inden for både oplysning, tekniske foranstaltninger samt regelbaserede tiltag.

Side 6/14

6.1 Oplysning

Ved oplysning forstås den samlede pulje af aktiviteter, hvormed man får kontakt til og forøget viden om emnet hos de involverede parter. Aktiviteterne kan for eksempel bestå i websites, kampagner på fjernsynet, i skoler og på fritidshjem eller konkurrencer. Oplysning er ikke én enkelt aktivitet, men derimod en bredt dækkende metode til at give børn og forældre viden om egen situation, så de får mulighed for at bedømme konsekvenserne af deres handlinger.

Sikkerchat.dk er et oplysningssite om online-sikkerhed for børn og unge. Sitet er et samarbejde mellem Red Barnet og Det Kriminalpræventive Råd og henvender sig til børn, unge og deres forældre.

<http://www.sikkerchat.dk>

Ved at give balanceret og relevant oplysning bidrager man til en sikker og ansvarlig internetbrug samtidig med, at man ikke lukker for børns adgang til at bruge internettet.

Som det ses af karakteristika for misbrugssituationerne handler en beskyttelse af børn og unge i høj grad om at gøre dem vidende om konsekvenserne af deres egne handlinger. Da de voksne sjældent lyver om deres alder eller deres hensigter er det vigtigt, at børnene forstår, hvad der kan ske, hvis de indgår i dialog med disse voksne, endsige mødes med dem. Ligeledes skal forældrene involveres i dialogen, da forældrene selv – gennem opmærksomhed og deltagelse i barnets digitale liv – kan forebygge mange af disse problemstillinger. Oplagte kanaler til at nå børn og unge er skoler og fritidsinstitutioner. Der findes allerede et stort materiale omkring web-etik til undervisningsbrug, og kampagner som ”Sikker

chat” har højnet opmærksomheden på området. Problematikken omkring oplysninger og privatlivets fred er tillige en del af It-sikkerhedskomiteéns fokus samt et af tre hovedemner for Netsikker Nu! kampagnen 2008.

Oplysningsindsatsen bør fortsætte, såfremt hele problematikken i misbrugssituationerne skal adresseres.

6.2 Tekniske tiltag

Et teknisk tiltag kan implementeres på forskellige måder. Det centrale i det tiltag, man vælger, er en balance mellem nytteværdien og konsekvenserne af den funktionalitet, der implementeres. Overordnet kan man tale om tre typer af funktionalitet: Verifikation, autentifikation og identifikation.

Verifikation er den helt simple form for kontrol. For eksempel kan man kontrollere, om nogle givne oplysninger er en adresse ved at se på, om de indeholder et vejnavn, et vejnummer, et postnummer og en by. Med andre ord betyder verifikation i sin simple form blot, at oplysningerne er dem, man at blevet bedt om – at man ikke opgiver sit navn, når man bliver bedt om adressen.

IT- og Telestyrelsen

Side 7/14

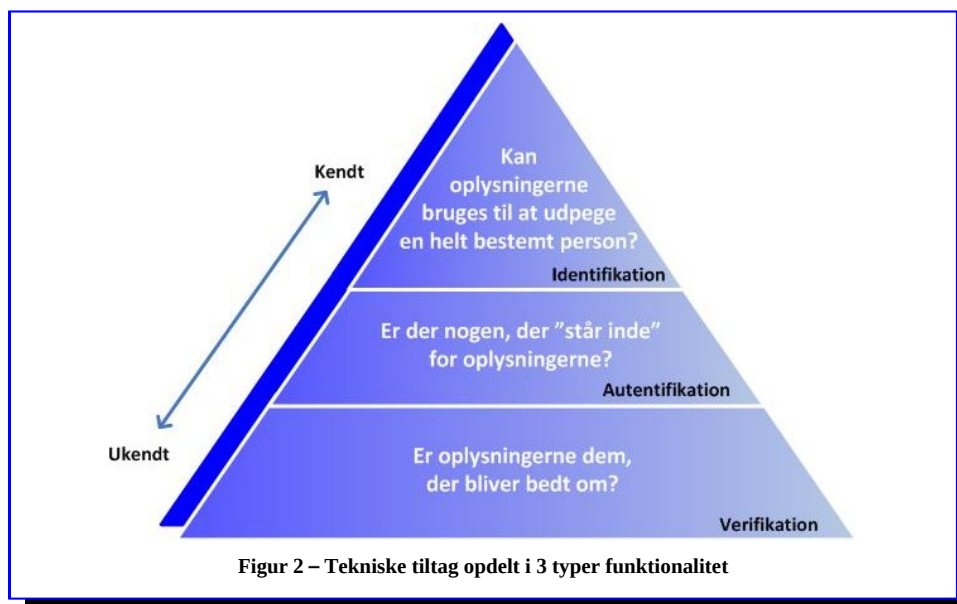
De fleste online sociale tjenester anvender i dag verifikation. Man kan kun få en profil på Facebook, hvis man er 13 år eller derover. Facebook verificerer, at det fødselsår, man har indtastet angiver en minimumsalder på 13 år. Men Facebook kontrollerer ikke, om det er rigtigt, at vedkommende bruger virkelig er 13 år. En 12-årig kan sagtens lave en profil på Facebook og sætte sit fødselsår et år tilbage.

Autentifikation tager verifikation skridtet videre og kræver en form for godkendelse – også kaldet validering – af, at de givne oplysninger er rigtige. For at genbruge analogien til en adresse, er det ved autentifikation ikke nok, at man angiver et vejnavn, et vejnummer, et postnummer og en by. Det skal valideres, at det er en adresse, der faktisk eksisterer. Validering sker typisk via en tredjepart. Det vil sige at der er nogen, der vil ”stå inde” for oplysningerne. For eksempel kan man forestille sig, at Kort- og Matrikelstyrelsen kan godkende, at en given vej eksisterer i Danmark ved at se, om de har oplysningerne registret i deres systemer. Validering via tredjepart kræver som udgangspunkt, at man har tillid til tredjepart.

Der arbejdes på teknologiske løsninger kaldet ”blind eller double blind certificates” så man ikke behøver at have tillid til tredjepart for at kunne validere givne oplysninger. Teknikken er dog ikke helt forfinet endnu, og kræver investeringer i udstyr og infrastruktur før den kan bruges i Danmark.

Identifikation etablerer entydigt identiteten på et individ. Som ved autentifikation skal det valideres, at personen eksisterer – man skal på baggrund af de givne oplysninger kunne udpege én helt bestemt person. Identifikation bruges i dag allerede i høj grad ved de digitale løsninger udbudt af det offentlige for eksempel ved anvendelse af den digitale signatur. Også bankerne anvender identifikation ved brugen af net-ID til login på web-bankerne.

Identifikation adskiller sig markant fra verifikation og autentifikation ved, at der *altid* er tale om en helt bestemt person. Ved både verifikation og autentifikation behøves man ikke at vide, *præcist* hvilken person, der er tale om. Man kan for eksempel godt både verificere og autentificere at en person er 14 år, uden at skulle vide *præcis* hvem personen er.



Figur 2 skitserer på funktionelt niveau ovennævnte tre typer af tekniske tiltag:

	Verifikation	Autentifikation	Identifikation
Validering af informationer		✓	✓
Mulighed for pseudonymitet / anonymitet	✓	✓	
Mulighed for identifikation / sporbarhed		✓	✓

Tabellen opsummerer de tekniske forskelle på de tre typer funktionalitet:

Teknisk kan man kun delvis adressere problematikken i misbrugssituationerne. Man kan aldrig helt forhindre kontakten mellem barn og voksen, men man kan beskytte børnene ved at give dem størst mulig valgfrihed i forhold til deres kommunikation med de voksne.

Det hjælper ikke at indføre tvungen identifikation på tjenesterne, som det for eksempel har været tænkt med brugen af digital signatur. I og med at de voksne som udgangspunkt ikke lyver overfor børnene, opnås blot, at barnets identificeres overfor den voksne. Herved får den voksne nemmere ved at finde barnet i den fysiske verden. Det er vigtigt, at barnet får muligheden for at være anonym. Samtidig skal man kunne stole på de oplysninger, der afgives.

Verifikation godkender ikke oplysningerne. Desuden er det ved brug af verifikation ikke altid muligt at spore en person bag en given profil. Dette medfører, at upassende opførsel på online sociale tjenester bliver risikofrit, da det ikke er muligt ved hjælp af tekniske hjælpemidler at finde den ansvarlige person. Problemstillingerne i verifikation understreges af, at problemet vedrørende misbrug stadig eksisterer, trods at de fleste online sociale tjenester anvender verifikation.

Et ungdomsbevis, det vil sige en teknisk foranstaltning børnene kan bruge i deres anvendelse af online sociale tjenester, bør teknisk bygge på funktionalitet, der giver børnene størst mulig valgfrihed. Valgfrihed skal sikre, at børnene får mulighed for beskytte deres privatliv ved selv at vælge, hvor meget information om sig selv de vil afsløre samtidig med, at de kan vælge at kommunikere med bestemte grupper af personer, eksempelvis børn mellem 12 og 14 år. Én måde at gøre dette på er ved at basere ungdomsbeviset på autentifikation. Herved valideres oplysninger, uden at barnets identitet afsløres. Dette medvirker til at opretholde balancen mellem teknisk at ville implementere tiltag til beskyttelse af barnet samtidig med, at barnets rettigheder overholdes og privatlivet i øvrigt respekteres. Skulle barnet opleve upassende opførsel, er det muligt at anmelde modparten – og ved et sammenspil mellem tjenesten, barnet og dem, der godkender oplysningerne – at finde frem til identiteten på den pågældende.

IT- og Telestyrelsen

Side 9/14

Et ungdomsbevis, der bygger på autentifikation, giver børnene større valgfrihed med hensyn til, hvem de vil snakke med. Børnene kan eksempelvis få en validering af, at modparten falder indenfor et givent aldersinterval. Autentificering via alder kan også give tjenesteudbyderne mulighed for at tilbyde fora, hvor kun personer, der har en bestemt alder eller aldersinterval, har adgang. Hermed kan børnene *vælge*, hvor gammel modparten skal være – uden på

Et ungdomsbevis, der bygger på autentifikation garanterer ikke, at børn ikke taler med voksne online. Konsekvenserne af hvem børnene taler med, og hvad de siger, kan kun forebygges gennem en oplysningsindsats.

Men med et ungdomsbevis, der bygger på aldersautentifikation kan børnene *vælge* aldersgruppen på dem, de vil tale med. Og dem, de har talt med, kan spores.

forhånd at afsløre andre informationer om sig selv end, hvor gammel man selv er. Et barn kan herved godt kalde sig Hans1234 på internettet og ifølge sin profil bo i Tønder, selvom han i virkeligheder hedder Peter og kommer fra København. Blot vil pseudonymet⁷ Hans1234 have samme alder som virkelighedens Peter. Barnet bestemmer således selv, hvor mange personlige oplysninger, det vil fortælle om sig selv.

Ønskes det på nuværende tidspunkt at implementere tekniske tiltag for at imødegå misbrugssituationerne, bør valget falde på autentifikation som funktionalitet. Verifikation stiller ikke børnene bedre, end situationen er i dag, tværtimod har de fleste tjenester allerede en form for verifikation implementeret. Identifikation på tjenesterne fratager børnene muligheden for selv at vælge, om

⁷ Et pseudonym er et opdigtet navn brugt af et givent individ for at skjule hans eller hendes rigtige identitet.

de vil oplyse, hvem de er i virkeligheden – dels til hinanden, men også til tjenesteudbyderen. Det vil være en klar overtrædelse af børnenes ret til privatlivet fred.

6.3 Regelbaserede tiltag

Regelbaserede tiltag kan implementeres på to måder: Ved lovgivning eller ved selvregulering.

Ved lovgivning kan stilles krav om, at udbyderne af online sociale tjenester implementerer en given funktionalitet, for eksempel at alle skal identificere sig med digital signatur på online

Chatmærket er et eksempel på et selvregulerende tiltag. Det udstedes af Chatmærkeudvalget, som består af repræsentanter fra FDIM, Red Barnet, Det Kriminalpræventive Råd, Arto og Egmont Serieforlaget. Chatmærket er i dag implementeret på Arto.dk, og er i gang med at blive implementeret på andre tjenester.

Lovgivning, der kræver identifikation på alle online sociale tjenester, krænker børns ret til privatlivets fred. Desuden kan tvangselementet medføre, at flere vil flytte deres kommunikation til udenlandske tjenester, som danske tiltag har sværere ved at påvirke.

sociale tjenester. Lovgivning er ikke egnet til at beskytte børn på disse typer tjenester, da børnene kan vælge at bruge udenlandske tjenester som MySpace og Facebook, der ikke er underlagt dansk lov.

Et alternativ til regulering ved lov er selvregulering. Tjenesteudbyderne har fordel af selvregulering, da de opnår troværdighed ved selv at iværksætte tiltag samt har indflydelse på udformningen af regelsættet. I øvrigt kan selvregulerende tiltag, der ikke er tilknyttet en specifik lov,

hurtigt tilpasses til forholdene på markedet.

Et væsentligt forhold, der taler imod selvregulering, er spørgsmålet om tjenesteudbydernes villighed til at adoptere og implementere regelsættet. Det kan ikke garanteres, at hele branchen vil benytte regelsættet. Der vil være mulighed for at omgå regelsættet på danske tjenester og som ved lovindgreb også på udenlandske tjenester, da det næppe er realistisk at forvente selvregulerende tiltag på internationalt niveau.

På trods af disse forbehold risikerer selvregulerende tiltag ikke at kompromittere børnenes ret til privatlivets fred i samme grad som direkte lovindgreb. Baseret på dette hensyn vil frivillige, brede aftaler i branchen bedst kunne tilgodese både beskyttelse af barnet, samtidig med at retten til privatliv bibeholdes.

7 anbefalinger

Analysen viser, at situationen omkring misbrug af børn som følge af dialog initieret på online sociale tjenester er kompleks. Anbefalinger må derfor findes indenfor både oplysning, tekniske samt regelbaserede tiltag.

7.1 Oplysning

Skal situationer, hvor der kan opstå misbrug, forebygges, må der bygges videre på den oplysningsindsats, som allerede pågår i samfundet.

EU spiller en stor rolle med centrale fælleseuropæiske initiativer til beskyttelse af børn i online-verdenen. Det nuværende program til fremme af en sikrere brug af internettet er iværksat af EU-kommissionen i 2005 under titlen ”Safer Internet Plus”. Der er i Danmark under denne paraply igangsat en række aktiviteter:

- Red Barnets internet-hotline mod pornografi og overgreb mod børn.
- Rigspolitiet har iværksat en række initiativer med henblik på at efterforske og retsforfølge strafbare forhold i forbindelse med ”grooming”.
- Internetudbydere har fastlagt en frivillig branchekodeks, der beskriver internetudbydernes procedurer for fjernelse af blandt andet børnepornografi på internettet.
- IT-Brancheforeningens ISP-kreds (Internet Service Providers) har etableret et forum, hvor også offentlige instanser deltager. Her udveksler internetudbydere viden og erfaringer.
- Videnskabsministeren tog i 2007 initiativ til, at branchen bag chatportalerne i Danmark samt andre relevante aktører etablerede en frivillig ordning, der har til formål at sikre, at udbydere af chatportaler understøtter en god web-etik for børn og unge, det såkaldte Chatkodeks. Chatmærket blev udviklet i 2006 på denne baggrund.
- Red Barnet og det Kriminalpræventive Råd har udarbejdet en informationskampagne ”Sikker chat”, der har til formål at informere teenagebørn og begyndere på internettet om de forholdsregler, som de bør tage, når de chatter på internettet.
- Medierådet for Børn og Unge har udarbejdet en informationskampagne, der henvender sig til børn, unge, forældre og lærere.
- IT- og Telestyrelsen har indledt samarbejde med UNI-C og Medierådet for Børn og Unge om web-etik for børn og unge for at informere lærere og elever om forholdsregler, som børn og unge bør tage, når de færdes på nettet.

IT- og Telestyrelsen

Side 11/14

Ovenstående er blot nogle eksempler på de aktiviteter og initiativer, der iværksættes på oplysningsområdet til at fremme sikker adfærd og viden om tjenester på nettet. Nærværende analyse påpeger, at oplysning er den primære indsats til at gøre noget ved den komplekse problematik, der knytter sig til de misbrugssituationer, hvor online kontakt fører til overgreb på børn.

7.2 Tekniske tiltag

Analysen viser også, at selvom tekniske tiltag kun kan yde delvis beskyttelse af børn på online sociale tjenester, er der muligheder på området. Teknisk set kan børn udstyres med et valg, så de får nogle kriterier til at bestemme, hvem de vil snakke med online. Dette kan ske uden, at børnene skal afgive flere personlige oplysninger, end de selv ønsker. Det anbefales derfor, at der ses nærmere på produkter og muligheder inden for autentifikation, for eksempel af alder.

7.3 Regelbaserede tiltag

Indsatsen, både på oplysningsområdet og tekniske tiltag, bør baseres på frivillighed. Ved lovgivning risikerer man, at børnene forsvinder til udenlandske tjenester, som tiltag fra nationalt hold ikke har mulighed for at påvirke.

En måde at styrke den frivillige indsats og koordinering på kan være etableringen af en tværgående koordinering af indsatsen. Videnskabsministeren har i 2007 taget initiativ til at nedsætte et tværministerielt embedsmandsudvalg, som er ved at færdiggøre en rapport, som giver et overblik over den hidtidige indsats til bekæmpelse af børnepornografi på internettet, herunder øvrige initiativer vedrørende børns sikkerhed på internettet generelt. Herudover skal udvalget overveje mulighederne for at iværksætte yderligere fælles eller ressortspecifikke initiativer, hvor overvejelser vedrørende koordination af viden og initiativer er en naturlig central del. Udvalgets endelige rapport forventes offentliggjort i efteråret 2008.

IT- og Telestyrelsen

Side 12/14

Bilag 1: Referenceliste

- Adam Theirer, 2007. "Social Networking and Age Verification: Many Hard Questions; No Easy Solutions". The Progress Freedom Foundation.
<http://www.pff.org/issues-pubs/pops/pop14.5ageverification.pdf> (tilgået 10. september 2008).
- Anick Jesdanun, 2006. "Age verification at social-network sites could prove difficult. USA Today", July, 2006.
- Barne- og Ligestillingsdepartementet, 2001. "Tiltaksplan, Barn, unge og internett".
<http://www.regjeringen.no/upload/kilde/bfd/bro/2001/0014/ddd/pdfv/136845-internettvern.pdf> (tilgået 10. september 2008).
- Crimes Against Children Research Center, 1999. "Youth Internet Safety Survey", (YISS-1). University of New Hampshire,
http://www.unh.edu/ccrc/projects/second_youth_internet_safety.html (tilgået 10. september 2008).
- Crimes Against Children Research Center, 2005. "Youth Internet Safety Survey", (YISS-2). University of New Hampshire,
http://www.unh.edu/ccrc/projects/youth_internet_safety_survey.html (tilgået 10. september 2008).
- David Randall and Victoria Richards, 2008. "Facebook can ruin your life. And so can MySpace, Bebo",
<http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-can-ruin-your-life-and-so-can-myspace-bebo-780521.html> (tilgået 10. september 2008).
- Det Kriminalpræventive Råd, 2002. "Overgreb mod børn, 2002".
- European Commission, 2007. "Safer Internet for Children, Qualitative Study in 29 European Countries. National Analysis: Denmark". Directorate-General Information Society and Media.
- Facebook. "Anvendelsesvilkår". <http://www.facebook.com/terms.php> (tilgået 10. september 2008).
- FDIM. "Chatmærket". <http://www.fdim.dk/?pageid=48> (tilgået 10. september 2008).
- Giles Hogben, 2007. "Security Issues and Recommendations for Online Social Networks", ENISA Position Paper No. 1.
- Helene Almind Jansen, 2008. "Den digitale børnelokker". Information 26. juli 2008.
- Home Office, 2005. "Home Office Task Force on Child Protection on the Internet".
<http://police.homeoffice.gov.uk/publications/operational-policing/search-and-advice-public.pdf> (tilgået 10. september 2008).
- iKeepSafe, Symantec, TRUSTe, 2007. "Online Privacy, A tutorial for Parents and Teachers",
http://www.truste.org/pdf/parent_teacher_tutorial.pdf (tilgået 10. september 2008).
- IT-borger.dk, 2008. "Sikkerhedsrisici ved sociale netværkstjenester", <http://www.it->

IT- og Telestyrelsen

Side 13/14

borger.dk/sikkerhed/virus-phishing-og-spyware/sociale-netverkstjenester

(tilgået 10. september).

Jakob Albrecht, 2008.

"Isenesat journalistik". Journalisten, juni 2008.

Janis Wolak et al., 2004.

"Internet-initiated Sex Crimes against Minors: Implications for Prevention Based on Findings from a National Study". Journal of Adolescent Health, volume 35.

Janis Wolak et al., 2006.

"Online Victimization of Youth: Five Years Later".

<http://www.unh.edu/ccrc/pdf/CV138.pdf> (tilgået 10. september 2008).

Kim Cameron, 2005.

"The Laws of Identity".

Malene Charlotte Larsen,
2008.

"Børn og unges liv i sociale mødesteder på internettet". Medierådet.

http://andk.medieraadet.dk/upload/boern_og_unges_liv_i_sociale_moedesteder.pdf (tilgået 10. september 2008).

OnGuard Online, 2007.

"Social Networking Sites: A Parent's Guide",

<http://www.onguardonline.gov/topics/social-networking-sites.aspx>

(tilgået 10. september 2008)

IT- og Telestyrelsen

Side 14/14

Red Barnet, 2006.

"Fra kigger til krænker? Om IT-relaterede seksuelle overgreb på børn".

Rigshospitalet, Team for
Seksuelt Misbrugte Børn,
2007.

"Statusrapport 2006-2007".