

## Nej til Big Brother mod terror

**EU-borgere er kritiske over for sikkerhedsteknologier som tilsidesætter privatlivets fred viser undersøgelse**

### Skeptiske borgere

- > **En interviewundersøgelse med i alt 180 deltagere i seks EU-lande peger i retning af, at borgerne i EU er mere skeptiske end deres politikere, når det gælder overvågning for at forhindre terror. De fleste af deltagerne så ikke at terrortruslen i sig selv var grund nok til at krænke privatlivets fred.**

### Dokumentation af effekt ønskes

- > **Hvis sikkerheden skal øges på bekostning af privatlivets fred, stiller borgerne høje krav til begrundelserne for overvågning – det skal dokumenteres, at det virker, og dommerkendelser skal ligge til grund for at bryde den beskyttelse af privatlivets fred, der ellers ligger i lovgivningen.**

### Tillid til myndigheder både-og

- > **De danske deltagere i undersøgelsen har – ligesom de norske – mere tillid til de offentlige myndigheder end de øvrige deltagere. Det betyder dog ikke, at de i højere grad accepterer øget overvågning af hensyn til sikkerheden.**

*Dette nyhedsbrev er skrevet på baggrund af rapporten "Synthesis report: Interview Meeting on Security Technology and Privacy", offentliggjort i november i projektet PRISE beskrevet i faktaboks på side 2 i nyhedsbrevet.*

Mens både EU og nationale parlamenter i disse år åbner for øget overvågning og registrering af borgere, så er almindelige mennesker overraskende kritiske og lader sig tilsyneladende ikke påvirke af den voksende terrorfrygt, der har præget den store politiske scene siden 11. september 2001.

Således mente et stort flertal af deltagerne i PRISE-projektets interviewmøder (se faktaboks), at brug af nye overvågningsteknologier, der griber ind i privatlivets fred, ikke kan retfærdiggøres med henvisning til truslen fra terror.

Undersøgelsen peger også på at kriminalitet er et bedre argument for overvågning end terror. Det vil sige at hensynet til at forhindre eller opklare alvorlige forbrydelser - opfattes som vigtigere end at forhindre terror, når det gælder om at forsvare brug af ny sikkerhedsteknologi.

For den almindelige borger i EU virker terrortruslen tilsyneladende ikke så påtrængende. Eller de

tror ikke på, at terror kan forebygges på lige den måde, som sikkerhedsteknologier lægger op til. Tendensen ses ikke mindst i Spanien, der har levet med terror i 30 år, og som med togbomberne i Madrid for få år siden oplevede et af de værste terrorangreb i Europa.

Resultaterne bygger på en serie såkaldte "interviewmøder" i seks lande: Danmark, Norge, Ungarn, Spanien, Tyskland og Østrig – udført af Teknologirådet i Danmark og teknologivurderingsinstitutioner i de øvrige lande.

Metoden er udviklet af Teknologirådet i Danmark til at opnå viden om, hvordan grupper af almindelige mennesker opfatter komplekse teknologier. Den kombinerer kvalitative gruppediskussioner med individuelle spørgeskemaer og er derfor egnet til at give et mere nuanceret billede end gængse opinionsundersøgelser.

Udgiver

Teknologirådet  
Antonigade 4  
DK - 1106 København K  
Tel. 33 32 05 03  
rtt@tekno.dk

Abonnement

Gratis pr. email  
Tilmelding på:  
rtt@tekno.dk  
Tidligere nyhedsbreve findes på:  
www.tekno.dk/rtt.htm

ISSN: 1602-4311

PRISE - projektet – det står for Privacy and Security - er betalt af EU med henblik på at udvikle "acceptable og accepterede" retningslinjer for sikkerhedsindustrien i Europa og for den tilhørende politik vedrørende sikkerhed vs. privatliv.

## PRISE

PRISE (PRIVacy and SEcurity) skal formulere et sæt af retningslinjer for udviklingen af sikkerhedsteknologi til brug for EU-kommissionen. Kommissionen har i 7. rammeprogram afsat midler til forskning og udvikling af sikkerhedsteknologier, med forventning om at sikkerhedsindustrien vil være et særligt betydningsfuldt område fremover. PRISE-projektet skal søge at imødegå potentielle konflikter mellem nye sikkerhedsteknologier og privatlivets fred, som er en af de fundamentale borgerrettigheder i demokratiske samfund.

## Status på projektet

Grænserne for privatlivets fred og borgerrettigheder er blevet kortlagt i to faser:

*Lovgivnings- og menneskerettighedsmæssige* begrænsninger for sikkerhedsteknologi er blevet beskrevet. Disse begrænsninger er ofte relateret til problematikker om indsamling, opbevaring og behandling af persondata.

*Holdninger til privatlivets grænser* er blevet afdækket gennem en række af *interviewmøder* – en metode udviklet af Teknologirådet. Borgerne i seks europæiske lande er blevet indbudt til at debattere og vurdere mulige måder at bruge nye sikkerhedsteknologier på. Rapporter fra de nationale møder er efterfølgende blevet samlet i en international rapport. Denne samlede rapport fra borgerinddragelsen tilfører projektet en bredere forståelse af hvad der betragtes som krænkelse af privatlivets fred, som ikke er begrænset til juridiske spørgsmål og spørgsmål om behandling af persondata.

Projektet afrundes med en konference i Wien i april 2008, hvor interessenter vil diskutere og perspektivere PRISE og med en bog, der vil opsamle de væsentlige bidrag i PRISE.

## Partnere

PRISE varetages i samarbejde mellem fire europæiske organisationer, der har erfaring med teknologivurdering: *Institut für Technikfolgen-Abschätzung i Øststrig*, *Teknologirådet* i Norge, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* i Tyskland og endelig *Teknologirådet* i Danmark.

## Læs rapporten om resultater af interviewmøderne

(engelsk):

[http://www.tekno.dk/pdf/projekter/prise/p07\\_PRISE\\_security\\_report\\_citizensmeeting\\_uk.pdf](http://www.tekno.dk/pdf/projekter/prise/p07_PRISE_security_report_citizensmeeting_uk.pdf)

## Læs rapporten fra det danske interviewmøde:

[http://www.tekno.dk/pdf/projekter/prise/p07\\_PRISE\\_security\\_report\\_borgermoede\\_dk.pdf](http://www.tekno.dk/pdf/projekter/prise/p07_PRISE_security_report_borgermoede_dk.pdf)

Undersøgelsen viser, at et stort flertal af de 180 deltagere fra seks forskellige lande vægter princippet om privatlivets fred meget højt, og at de føler ubehag ved overvågning. Hvis de skal acceptere øget overvågning til gengæld for øget sikkerhed, stiller de høje krav, både til begrundelserne for overvågning og til måden den udføres på.

For at en overvågning anses for rimelig, skal der være tydelig proportionalitet mellem mål og middel. Det skal stå klart, at en given form for overvågning rent faktisk vil øge sikkerheden på et konkret område. Samtidigt skal alternative muligheder altid overvejes. Altså om samme grad af sikkerhed kan opnås med andre midler.

Kort sagt: Sikkerhedsteknologien skal være dokumenteret effektiv. Og indgrebet i privatlivet skal kunne retfærdiggøres af den trussel, som det drejer sig om. Det er ikke nok med vage formuleringer om terrorbekæmpelse.

## Mistillid til myndighederne

Interviewmøderne viste også, at et stort flertal af deltagerne i de 6 lande nærer mistillid til myndighederne - i retning af at overvågningsteknologierne nok alligevel vil blive indført uden tilstrækkelig begrundelse. Samt at en teknologi, når den først er indført, vil være umulig at slippe af med – selv hvis det viser sig, at den ikke virker efter hensigten.

90 procent af deltagerne følte sig overbevist om, at overvågnings-teknologierne vil blive misbrugt. Enten af kriminelle – og af virksomheder i kommercielt øjemed. Mens 60 procent mener, at også myndighederne vil misbruge overvågningen.

På dette punkt viser undersøgelsen store udsving, og peger på store forskelle i borgernes tillid til myndighederne i de forskellige lande. Danskerne og nordmændene har størst tillid, mens ungarerne ligger i bund. Tyskerne udmærker sig ved at være meget kritiske og mistroiske med hensyn til registre og dataopbevaring. Her spiller landenes historie og erfaringer med statens overvågning af borgerne tydeligt ind.

## Fare ved den menneskelige faktor

I alle lande er borgerne bekymrede over "den menneskelige faktor" - altså at teknologien kan misbruges af enkeltpersoner, eller at følsomme data slipper ud på grund af menneskelige fejl. Deltagerne lagde stor vægt på, at der gøres så meget som muligt for at undgå, at teknologien misbruges.

Borgerne i undersøgelsen har også massivt fokus på faren for "function creep" – "glidebaneeffekt" – dvs. at en given sikkerhedsteknologi eller data indsamlet med et særligt formål – pludseligt bruges i en anden sammenhæng end det oprindeligt var tiltænkt.

Undersøgelsen giver omvendt det indtryk, at man kan vænne borgerne til overvågning, hvis teknologier er så meget tilstede i det offentlige rum, at man

## Udgiver

Teknologirådet  
Antonigade 4  
DK - 1106 København K  
Tel. 33 32 05 03  
rtt@tekno.dk

## Abonnement

Gratis pr. email  
Tilmelding på:  
rtt@tekno.dk  
Tidligere nyhedsbreve findes på:  
www.tekno.dk/rtt.htm

ISSN: 1602-4311

ikke længere lægger mærke til den. Desuden er der større accept af overvågning i det offentlige rum, end i privatsfæren. Det forklarer blandt andet den relativt høje accept af for eksempel videoovervågning.

## Sikkerhedsteknologier

Undersøgelsen drejer sig om sikkerhedsteknologi inden for syv hovedområder.

**1. Biometriske målinger.** Teknologi der kan identificere personer ud fra deres biologiske karakteristiske eller deres måde at bevæge sig på. Det kan være fingeraftryk, ansigtsmålinger, irisgenkendelse. Målingerne kan bruges ved id-papirer, såsom pas, ved adgangskontrol, men også til identifikation på computere med følsomme dokumenter.

**2. Kameraovervågning.** Aktive kameraer kan følge enkeltpersoner over større afstande. Og computerprogrammering kan få kameraerne til at følge personer med påstået "mistænkelig adfærd". Det kan også bruges ved trafikovervågning, f.eks. overtrædelse af hastighedsgrænser

**3. Scanninger.** F.eks. med røntgen eller med *terahertz*, der kan afsløre, hvad folk har under tøjet. "Nøgenmaskinen" viser alt, hvad der findes under tøjet. Andre systemer affotograferer skjulte genstande, og projicerer dem op på en kønsløs mannequin-dukke.

**4. Positioneringsteknologi:** At følge en persons færden ved hjælp af mobiltelefonnettet – eller ved hjælp af GPS-sendere. eCall teknologien i biler, kan programmeres til at ringe op til en central, hvis der sker en ulykke. Men der er frygt for, at den – hvis den bliver standardudstyr i nye biler – vil kunne aktiviseres til andre formål.

**5. Aflytning.** Af fastnet eller mobiltelefon. Et af spørgsmålene er, om man kun må aflytte en mistænks telefon eller også de personer, den mistænkte taler med.

**6. Opbevaring og brug af data-registre.** Ved at sammenføre registre kan man få omfattende informationer om enkeltpersoner. Tendensen i Europa går i retning af at koble informationer og gøre dem tilgængelige på tværs af grænserne.

**7. Privatlivs-fremmende teknologier,** f.eks. kryptering af e-mails, kryptering af telefonsamtaler eller brug af anonymiserende telefonkort, eller deltagelse i anonyme diskussionsfora på internettet.

Hertil kommer en klar tendens til at acceptere sikkerhedsteknologien i særlige 'farezoner'. For eksempel i byområder hvor risikoen for kriminalitet - overfald eller tyveri - er høj. Eller steder hvor, hvor risikoen for terror anses for høj. I lufthavne er de fleste villige til at acceptere næsten enhver form for sikkerhedsteknologi.

90 procent accepterer således videoovervågning i lufthavne, mens over halvdelen accepterer videoovervågning på stationer, ved banker og i sportsarenaer.

En nationalitet skilte sig dog ud på dette punkt. De 33 deltagere i det spanske borgermøde havde tendens til at være mere kritiske over for sikkerhedsteknologi og brugen af den, jo mere de kendte til den.

## Nej til nøgen-maskinen

Ser man på de enkelte teknologier gælder det, at jo tættere de kommer selve den menneskelige krop, jo sværere er de at acceptere. Det gælder for eksempel ansigtsscanning med henblik på genkendelse og i mindre grad irismålinger af øjet.

Allerværst er det med den såkaldte "Naked Machine" – "Nøgenmaskinen" – der med en særlig røntgenteknologi, danner et detaljeret billede af kroppen og kroppens former under tøjet for herved at kunne afsløre enhver form for skjulte genstande. En maskinel erstatning for gammeldags kropsvisitering. Men den vækker meget stærk modstand.

Det samme gælder videoovervågning i omklædningsrum – for eksempel i butikker – der anses for krænkende, selv om netop videoovervågning generelt hører til blandt de mest accepterede former for overvågning.

## Nuancerede synspunkter

Undersøgelsen viser, at de fleste har en særdeles nuanceret tilgang til spørgsmålet om sikkerhedsteknologi vs. privatliv – og at flere informationer kan rykke deres opfattelser, også i retning af at acceptere teknologien.

Det gælder for eksempel de såkaldte lokaliseringsteknologier (f.eks. GPS-overvågning), der generelt anses for et stærkt indgreb i privatlivets fred. Men en påpegning af, at teknologien også kan bruges til at lokalisere forulykkede, var med til at mindske modstanden.

Nogle spørgsmål deler deltagerne. For eksempel om hvorvidt samfundets sikkerhed afhænger af sikkerhedsteknologien, og om en teknologi skal anvendes, hvis den er tilgængelig.

Der er også uenighed, når det kommer til spørgsmålet, om alle skal tvinges til at underkaste sig teknologien, hvis den bliver indført af virksomheder eller myndigheder.

Et flertal mener, at det ikke må få konsekvenser for den enkelte borger, hvis vedkommende er uvillig til at underkaste sig teknologien eller måske ikke kan

## Udgiver

Teknologirådet  
Antonigade 4  
DK - 1106 København K  
Tel. 33 32 05 03  
rtt@tekno.dk

## Abonnement

Gratis pr. email  
Tilmelding på:  
rtt@tekno.dk  
Tidligere nyhedsbreve findes på:  
www.tekno.dk/rtt.htm

ISSN: 1602-4311

bruge teknologien. Det kan være håndværkere, der i forbindelse med deres arbejde har mistet deres fingeraftryk. Men det kunne også være mennesker, der nægter at lade sig registrere i en database. Deltagerne i borgermøderne mente, at der skal være en grad af frihed til om man vil være med eller ej, også hvis det kan svække den generelle sikkerhed.

Generelt er der stor forståelse for, at brug af overvågningsteknologi i visse tilfælde kan være nødvendig. Men når det kommer til den konkrete brug, er der stor skepsis.

Diskussionerne bevægede sig mellem to grundsynspunkter, det kunne formuleres således:

”Hvis jeg ikke har noget at skjule, har jeg ikke noget at være bange for” – som stod over for:

”Hvis jeg ikke har noget at skjule, hvorfor skal de så overvåge mig?”

## Dommerkendelser og demokrati

Hvis det endelig skal være, så anses dommerkendelser for et godt redskab til at gøre det uacceptable acceptabelt. Det gælder for eksempel aflytning og GPS-overvågning – altså teknologier, der kan følge en persons færden. Her er tale om teknologier, som vurderes at gå meget tæt på den enkeltes privatliv, men som samtidigt anerkendes som særdeles nyttige redskaber for politiet. Uden dommerkendelse anses de for uacceptable.

Undersøgelsens deltagere formulerede også en række demokratiske anbefalinger i forbindelse med indførelse af sikkerhedsteknologier og sikkerhedsforanstaltninger:

Alle beslutninger skal baseres på åbne og gennemsigtige beslutningsprocesser - men endnu vigtigere: Før beslutningerne træffes, skal det gennemføres en offentlig debat, der involverer borgerne og giver dem den nødvendige information til at kunne debattere på et kvalificeret grundlag.

Desuden skal alle relevante interessegrupper, eksperter og menneskerettighedsorganisationer høres før enhver beslutning der berører spørgsmål om sikkerhed vs. privatliv.

Endelig skal hensynet til privatlivets fred have en fremtrædende placering hver gang et nyt sikkerhedsprojekt analyseres. På samme måde skal der kun gives penge til forskning i ny sikkerhedsteknologi, hvis det kan godtgøres at konsekvenserne for borgernes private liv analyseres til bunds.

*Fra Rådet til tinget udgives af Teknologirådets sekretariat. Redaktør Ida Leisner. Dette nummer er skrevet af Thomas Klenow With.*

### De sidste fem numre af Fra rådet til tinget:

Nr. 246: *Grundlag for prioriteringer skal frem i lyset*

Nr.245: *Energi for fremtiden*

Nr.244: *Åbne og aktive innovationsprocesser er nødvendige*

Nr. 243: *Lægeordineret heroin nu*

Nr. 242: *National strategi for biodiversitet nødvendig*

*Fra rådet til tinget stilles alene til rådighed for visning/læsning. Det er ikke tilladt at kopiere, hverken på papir, elektronisk eller i digital form. Der må dog tages kopi til egen personlig brug, jf. Ophavsretslovens § 12. Der må kun citeres med kildeangivelse og kun linkes til visninger på måder, der fører hen til Teknologirådets hjemmeside. Yderligere rettigheder til materialet kan aftales ved henvendelse til redaktør Ida Leisner.*

### Udgiver

Teknologirådet  
Antonigade 4  
DK - 1106 København K  
Tel. 33 32 05 03  
rtt@tekno.dk

### Abonnement

Gratis pr. email  
Tilmelding på:  
rtt@tekno.dk  
Tidligere nyhedsbreve findes på:  
www.tekno.dk/rtt.htm

ISSN: 1602-4311