VRAAG

Stap 1: Het sleepnet

Het voorstel
De regering wil dat de geheime diensten de mogelijkheid krijgen om in bulk communicatie te onderscheppen. Deze kunnen vervolgens gefilterd en doorzocht worden op mogelijk interessante informatie voor de geheime diensten.

ANTWOORD
Een van de taken van de overheid is de burgers te beschermen tegen criminaliteit. Dat vereist opsporing. Natuurlijk wenst de overheid daarom grotere toegang tot allerlei datastromen.

Het breed vergaren van data in dataverzamelingen schept echter grote nieuwe risico's die de burger bedreigen, zoals:

- Ambtenaren die legaal toegang hebben tot die dataverzamelingen, maar deze toegang buiten hun bevoegdheid gebruiken voor niet legitieme doelen. Ook dit is een vorm van criminaliteit.

- Personen die niet legaal toegang hebben tot die dataverzamelingen, maar op allerlei manieren ("vriendendienst"; frauduleus inloggen, hacken van systemen) toegang krijgen en die voor hun eigen doelen (goedbedoeld of kwaadaardig) gebruiken.

- Overheidsfunctionarissen of instellingen die buiten hun legale bevoegdheid hun ondergeschikten die wel legale toegang hebben verplichten om de data voor niet legitieme doelen te gebruiken (en zwijgplicht opleggen).

- In situaties van oorlog of onrust kunnen nieuwe (legitieme of illegitieme) machthebbers de data op allerlei manieren misbruiken. [denk aan bevolkingsregisters ten tijde van de bezetting '40-'45].

- Alle dataverzamelingen bevatten fouten; door foute invoer, foute data-analyse, menselijke vergissingen, kwaadwillendheid. De burger (en andere rechtspersonen en instellingen) kunnen nooit toegang hebben tot al de over hen vergaarde gegevens: het is gewoon veel te veel, niet systematisch te vinden, en voor een belangrijk deel vertrouwelijk. De ervaring met de WOB (Wet Openbaarheid van Bestuur) laat zien dat ook nu burgers grote moeite hebben met het verkrijgen van inlichtingen waarop ze recht hebben. Met zulke grote dataverzamelingen is een goede uitvoering van het recht on fouten te vinden en te laten corrigeren onmogelijk.

- Er ontstaat een nieuwe vorm van criminaliteit: het bewust verspreiden van valse informatie die door de data-vergaartechnieken wordt opgenomen, en de reputatie van betrokkenen grote schade kan toebrengen (o.m. onterechte verdenkingen).

- Het is een onbetwistbaar feit dat geen enkel IT systeem volledig veilig is tegen hacken. Het bestaan van deze dataverzamelingen opent de mogelijkheid dat buitenlandse staten en "non-state actors" inbreken en de data gebruiken voor hun eigen doelen, en daarmee de staatsbelangen en de burgers zwaar kunnen schaden of zelfs bedrijven.

- Alle nieuwe IT initiatieven neigen tot "Mission Creep". Voor alle massieve overheids-dataverzamelingen is er een groot gevaar dat de samenleving besluit om die data, geheel legaal, voor allerlei maatschappelijke doelen te gaan gebruiken. Maar alle IT systemen zijn kwetsbaar foor falen, door interne fouten (software updates), technische fouten (defecten, ongevallen, brand, enz.) of kwaadwillendheid van individuen zoals hackers, criminele groepen of buitenlandse staat- en niet-staat actoren. Daarmee introduceert men grote "afbreuk" risico's.

- Het blijkt steeds dat "hackers" van allerlei soort (personen, instituties, niet-staat en staat-actoren) meer kunnen ("aanval") dan de beheerders en gebruikers van data ("verdediging") verwachten. Lang niet elke inbreuk op systemen wordt bij de beheerders bekend. Grote dataverzamelingen geven dus een "aanvalsdoel" aan onze vijanden dat zij ongemerkt kunnen gebruiken en kwaadaardig wijzigen.

Deze opsomming van de risico's van overheids-dataverzamelingen is zeker niet volledig.

Het is geheel onverantwoord om enig initiatief te nemen om als overheid meer data te gaan vergaren of bestaande data in grotere bestanden te aggregeren zonder een degelijke analyse van alle nieuwe risico's die daardoor ontstaan, zowel voor individuele burgers of voor de samenleving in zijn geheel.

Al lang geleden heeft onze samenleving gekozen voor ons traditionele recht op "bescherming van de eigen levenssfeer" (privacy). Dat is natuurlijk een forse hinderpaal voor opsporing van criminaliteit, maar dat werd minder zwaar gewogen dan het alternatief dat verbroken privacy allerlei andere risico's voor de burger meebrengt.

Nu in het IT tijdperk moeten we dezelfde denkwijze blijven volgen, en zeer behoedzaam zijn met het opzetten van nieuwe databestanden.

VRAAG

Stap 2: Het verbeteren van het toezicht op de geheime diensten

Het voorstel
De regering stelt voor om het toezicht op de geheime diensten aan te scherpen. Als de minister besluit om iemand te tappen, kan de toezichthouder (de CTIVD) laten weten dat het onterecht is.

ANTWOORD
Machtmisbruik door een hooggeplaatste (Minister; hoofd van een dienst) is natuurlijk een risico. Slechts een klein deel hiervan kan worden uitgebannen door formele bezwaar- en beroepsprocedures. Een groot probleem is dat het uiterst moeilijk is om aan te tonen dat een wederrechtelijk besluit tot datavergaren is genomen, waartegen men zou kunnen klagen.

Ten tweede, al deze procedures zijn langzaam: minstens maanden, vaak jaren. Dan is de schade aan de persoons- of bedrijfsbelangen al lang onomkeerbaar. De benadeelde heeft nauwelijks baat met de procedure, zelfs als hij "wint".

Ten derde, al zou de procedure uitmonden in een rechterlijke uitspraak, dan is het nog niet zeker dat de overheid die gehoorzaamt [zie het recente oordeel in de Urgenda-klimaatzaak]. Ook bij uitspraak in hoger beroep is er geen enkel machtmiddel (behalve politiek) om uitvoering van het vonnis af te dwingen.

Het heeft daarom geen zin zich druk te maken over deze voorgestelde procedure. Het raakt alleen "het topje van de ijsberg", en het hele bestaan van de procedure kan men beschouwen als niet meer dan "Show voor de Bühne".

De enige manier om misbruik van databestanden te vermijden is te zorgen dat die bestanden niet bestaan. Burgers mogen er van uitgaan dat bij elk databestand elke vorm van misbruik zal voorkomen, als dat binnen de overheid als voldoende nuttig wordt beschouwd. Waarschijnlijk is misbrui door niet-bevoegden een groter risico.

VRAAG

Stap 3: Uitwisseling met buitenlandse geheime diensten

Het voorstel
De geheime diensten werken veel samen met buitenlandse geheime diensten om informatie met elkaar uit te wisselen. In de praktijk blijkt dat deze informatie in bulk gedeeld wordt.

ANTWOORD
Alle hierboven aangevoerde bezwaren gelden nog veel sterker als de dataverzamelingen in "rauwe" vorm worden gedeeld met het buitenland.

Daarbij komt nog:

- niet-legitieme toegang tot de data wordt nu volledig afhankelijk van de kwaliteit van datazekerheid van de betrokken buitenlandse diensten. Als data met de NATO worden gedeeld, is de beveiliging die van het minst beveiligde NATO land. Men mag eer niet op rekenen dat elk buitenland de Nederlandse dataverzamelingen even goed zal beveiligen als de eigen data.

- Data-uittreksels zullen in andere talen worden vertaald, misschien meermaals achtereen. Vertaalfouten (denk aan computervertalingen) kunnen tot totaal verkeerde conclusies leiden, die nauwelijks zijn te ontdekken of te herstellen.

- Data zal met buitenlandse data worden gekoppeld. Er is een aanzienlijk gevaar voor verkeerde koppeling (bijv. verwisseling van identiteit), met potentieel ernstige gevolgen.

- Handelingen van burgers die in Nederland legitiem zijn kunnen in andere landen strafbaar zijn. Het geldt niet alleen zaken zoals homoseksualiteit of overspel. Belangrijker is dat sommige staten - de VS. voorop - voor hun binnenlandse wetgeving "extraterritoriale werking" claimen. Zo kan een handelaar die in goederen handelt die vallen onder een Amerikaans boycot, bij een bezoek aan de VS worden vervolgd wegens overtreding van de boycot, met de kans op hoge straffen. Het leveren van data die we in Nederland "onbelangrijk / ongevaarlijk" vinden kan in het buitenland grote gevolgen hebben. Buitenlandse diensten weten dit, en kunnen via "datamining" dergelijke "extraterritoriale strafbare feiten" systematisch gaan zoeken. Het delen van data met buitenlandse diensten breng de veiligheid van Nederlandse reizigers in het buitenland in gevaar.