

Geachte meneer/mevrouw,

Onderstaande mijn reactie op het huidige wet voorstel. Ik wil vooral reageren op de mogelijke grootschalige onderschepping ('in bulk') van digitale communicatie.

Volgens het voorstel is de grootschalige onderschepping (een sleepnet) onmisbaar. Maar die onmisbaarheid lijkt niet goed onderbouwd, voor een ingreep die enorme consequenties heeft.

Het massaal verzamelen van communicatie van burgers op wie geen verdachting rust gaat tegen het principe van onze rechtstaat in, en het basis recht op privacy van ieder mens (Universele Verklaring van de Rechten van de Mens, 1948). Daarnaast is er het VN-verdrag voor Burgerlijke en Politieke rechten (1966) waarin staat:

- Niemand mag worden onderworpen aan willekeurige of onwettige inmenging in zijn privéleven, zijn gezinsleven, zijn huis en zijn briefwisseling, noch aan onwettige aantasting van zijn eer en goede naam.
- Een ieder heeft recht op bescherming door de wet tegen zodanige inmenging of aantasting.

Het recht op privacy is een belangrijk onderdeel van onze samenleving. Ieder mens moet door het leven kunnen gaan en communiceren, zonder zich over alles af te hoeven vragen of informatie niet automatisch door de overheid wordt onderschept, geanalyseerd, en opgeslagen. Dit is iets wat in het oude Oost Duitsland en de USSR geprobeerd werd, niet iets wat wij zouden moeten doen in onze eigen samenleving.

Naast de rechterlijke en principiële bezwaren, is het ook nog zeer de vraag of een sleepnet wel effectief is. De daders in twee high-profile zaken van het afgelopen jaar (Charlie Hebdo en de Thalys) hebben allemaal voor de aanslag (of poging tot) onder specifieke surveillance gestaan, maar dit heeft duidelijk niet geholpen. Waarom zou grootschalige onderschepping van informatie dan wel helpen? De kans dat het vangnet een daadwerkelijke crimineel kan oppikken, is waarschijnlijk klein. Daar bovenop is het triviaal om een digitaal vangnet te omzeilen voor een potentieel crimineel door encryptie te gebruiken, wat de kans op detectie nog kleiner maakt. Het zou daarnaast niet raar zijn als potentiële criminelen door het vangnet juist meer encryptie gaan gebruiken. De kans dat onschuldige mensen als 'gevaarlijk' worden gesignaleerd is daarentegen zeer reëel, gezien de hoeveelheid informatie die verzameld zou worden. Dit alles heeft tot gevolg dat een grootschalig en duur project vooral tot verdenking van in werkelijkheid onschuldige burgers zou leiden, en het zelfs moeilijker zou kunnen maken om daadwerkelijke criminelen te volgen.

Ondanks de consequenties van een digitaal vangnet, zijn de de risico's die met het vangnet voorkomen moeten worden relatief klein. De kans om door een terroristische aanslag om te komen is verwaarloosbaar vergeleken met vele andere oorzaken. Volgens het CBS zijn er bijvoorbeeld rond de 500 mensen in het verkeer omgekomen per jaar, terwijl het aantal terreur slachtoffers in Nederland op een aantal handen te tellen is.

De mogelijkheid tot afluisteren, aftappen en onderschepping zal altijd belangrijk zijn. Maar dit soort maatregelen moeten gericht genomen worden, op personen die onder redelijke verdenking staan en bij toestemming van een rechter. Massale ingrepen zoals het voorgestelde vangnet snijden teveel in de rechten van de mens, en geven te weinig uitzicht op betere resultaten.

Met vriendelijke groet,

Sander Keemink

swkeemink@scimail.eu

PhD Kandidaat Neurowetenschappen aan de University of Edinburgh

Nederlands Staatsburger