Reactie op de voorgestelde wet op de inlichten- en veiligheidsdiensten

Wesley Roozing

2015-09-01

Even voorstellen: Ik ben Wesley Roozing, een 26-jarige ingenieur bezig met een PhD in robotica. Ik heb een zeer grote affiniteit en kennis van technologie, digitale communicatie en het internet. De bescherming van privacy en bescherming tegen overheidssurveillance zijn onderwerpen die mij zeer dicht bij het hart liggen op een moment waar de capaciteit tot surveillance groter is dan ooit in de geschiedenis. Ik heb dan ook met zere ogen meegelezen tijdens de afgelopen 2 jaar naar mate er meer bekend werd over hoe ver overheidssurveillance, door zowel binnen- als buitenlandse diensten, momenteel al gaat. Daarom wil ik graag kort mijn mening - en de mening van vele anderen om mij heen - laten horen in deze consultatie.

Recentelijk is het voorstel voor een nieuwe wet op de inlichtingen- en veiligheidsdiensten bekend geworden. Het voorstel voor de nieuwe wet betreft 3 hoofdpunten:

- Massale onderschepping digitale communicatie middels sleepnet
- 'Verbeteren' van het toezicht op de geheime diensten
- Uitwisseling van informatie met buitenlandse geheime diensten

Van deze punten is de grootste wijziging t.o.v. de huidige situatie het sleepnet, waarbij ongericht alle communicatie van de burger mag worden afgetapt. Dit mag momenteel alleen gericht gebeuren. Dit is een grove inbreuk op de privacy, en bovendien ineffectief. De problemen met massasurveillance kom ik later in deze brief op terug.

Er wordt aangedragen dat het toezicht op de geheime dienst dan ook verbeterd wordt, echter in het huidige voorstel wordt de beslissing of een tap terecht is nooit bij de rechter neergelegd, maar bij politici. **Dit is regelrecht tegen de principelen van de rechtstaat.** Dit geldt tevens bij individuele taps, niet alleen bij het sleepnet.

Het derde punt, uitwisseling van informatie met buitenlandse geheime diensten, is een verdere inbreuk op de privacy. Buitenlandse geheime diensten kunnen zo massaal (ongefilterd!) informatie verzamelen over (onverdachte!) Nederlanders. Deze informatie is vervolgens overgeleverd aan de wetten van andere landen, en bovendien is er geen enkele garantie over hoe buitenlandse

diensten met deze data omgaan, zoals veelmaals is aangetoond in het geval van bv. de NSA en BND.

1 Problemen met massasurveillance

1.1 Privacy

Het voornaamste argument tégen massasurveillance is uiteraard privacy. Privacy is een recht, opgenomen in de Universele Verklaring van de Rechten van de Mens (1948). In artikel 17 van het VN-verdrag voor Burgerlijke en Politieke rechten uit 1966 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 mag duidelijk zijn dat massasurveillance als voorgesteld loodrecht op dit verdrag staat. Het monitoren van iemands gedrag op internet is één van de grofst mogelijke inbreuken op de prive sfeer van het individu, omdat men een bepaalde verwachting van privacy heeft: De diepste geheimen, fantasien en onzekerheden komen daar tot uiting omdat men die niet durft te bespreken met een ander persoon.

Bovendien wordt er inbreuk gemaakt op de privacy van bepaalde specifieke groepen mensen. Journalisten, klokkenluiders, dokters, advocaten en rechters, om er een paar te noemen. Voor het correct functioneren van een democratische rechtstaat is het vrij kunnen opereren van journalisten en klokkenluiders een **absolute vereiste**. Journalisten en klokkenluiders moeten misstanden van de overheid aan de kaak kunnen stellen zonder daarbij bang te zijn voor consequenties. Zie bijvoorbeeld WikiLeaks, Edward Snowden of Glenn Greenwald, of onze eigen Fred Spijkers, Paul van Buitenen of Ad Bos.

Een andere aspect van het belang van privacy is de invloed die het heeft op het gedrag van mensen. Het is intuïtief waar, maar tevens meermaals aangetoond in de sociale wetenschap dat de kennis dat men bekeken wordt het gedrag van mensen beïnvloedt. Dergelijke massasurveillance oefent dan ook een soort absolute macht uit op het volk, wat de machtsbelans tussen overheid & volk op de verkeerde voet zet.

1.2 Ineffectiviteit

Het argument dat gebruikt wordt bij maatregels als het sleepnet is doorgaans (georganiseerde) criminaliteit, kinderporno of, voornamelijk, terrorisme. Er zijn meerdere redenen waarom de effectiviteit van massasurveillance op zijn minst zeer twijfelachtig te noemen valt:

1. Surveillance voorkomt geen aanvallen. Recentelijk hebben er 2 (pogingen tot) terroristische aanvallen plaatsgevonden; Charlie Hebdo en de Thalys in België. In beiden gevallen waren de daders bekend bij de politie/geheime diensten maar in beiden gevallen heeft dit niets gebaat. In het geval van de Thalys heeft de heldhaftigheid van een paar toevallig aanwezige Amerikaanse mariniers een bloedbad kunnen vermijden. Ook de aanslag op de marathon in Boston is niet voorkomen ondanks het zeer verregaande afluisterbeleid van de VS.

2. Digitale communicatie is makkelijk te beveiligen - encryptie **werkt**. Goed geimplementeerde encryptiealgoritmen zijn betrouwbaar, gebaseerd op wiskunde die het voor een derde partij, hoe technologisch geadvanceerd ook, onmogelijk maakt om te breken. De gereedschappen hiervoor zijn vrij beschikbaar en niet moeilijk te gebruiken. Zonder in te gaan op te talloze mogelijkheden: iemand die iets wil verbergen, die **kan** dat. Dat betekent dat de mensen waarvoor deze wet bedoeld is om in te gaten te houden, met weinig moeite in staat zijn verborgen te blijven. Alle overige burgers worden wél geraakt.

De effectiviteit van dergelijke maatregelen is dus absoluut niet bewezen, en er zijn zéér sterke argumenten te maken tégen de effectiviteit.

1.3 Disproportionaliteit

Een enigszins macaber, maar realistisch, argument is dat de doden door terrorisme verwaarloosbaar zijn t.o.v. andere niet-natuurlijke doodsoorzaken. Het CBS heeft recent berekend dat er zo'n 500 mensen per jaar omkomen in Nederland in het verkeer. Sinds de 2e wereldoorlog heeft de grootste aanslag in Nederland 9 slachtoffers geëist, bij de acties van Molukkers in 1970. Tussen 1990 (aanslag van IRA in roermond waarbij 2 Australische toeristen omkwamen) en 2004 (Theo van Gogh) vielen er in Nederland geen doden bij terroristische aanslagen. Ter vergelijking, als we de 500 verkeersdoden per jaar extrapoleren naar 1970, komen we op zo'n 22.500 verkeersslachtoffers.

De risico's gevormd door terrorisme staan dan ook erg twijfelachtig tegenover de enorme inbreuk op privacy, tesamen met de enorme kosten van het verwerken en opslaan van de data.

1.4 Omgekeerde bewijslast

De opkomst van zeer krachtige computersystemen stelt entiteiten met voldoende middelen in staat om de enorme hoeveelheid data opgeslokt door een digitaal sleepnet te verwerken, zonder noodzakelijke tussenkomst van mensen. Men is overgeleverd aan algoritmen die 'risicovol' gedrag moeten oppikken. Door de gelimiteerde informatie die het systeem te verwerken krijgt, zal geautomatiseerde analyse van grootschalig opgevangen persoonlijke gegevens een volledig verkeerd beeld scheppen van personen. Echter, op dat moment is de bewijslast al wel

omgedraaid. Als het algoritme heeft besloten dat een bepaald persoon 'risicovol' is op basis van de opgevangen stukjes informatie, is het vervolgens aan deze persoon om te bewijzen dat hij/zij onschuldig is.

Het resultaat is tevens dat er veel valse positieven gegenereerd worden. Er valt een analogie te maken met een test op een ziekte; als de test een dergelijke grote hoeveelheid valse positieven oplevert is hij niet betrouwbaar en zal hij niet gebruikt worden. Het resultaat is dat er miljoenen mensen op 'terrorist watchlists' komen te staan zoals bv. het geval is in de VS, waar een dergelijke lijst 1.5 miljoen mensen bevat. Het gevolg daarvan zijn mensen die onterecht niet mogen vliegen, ongeterechte binnenvallen en arrestaties van mensen die toevallig de verkeerde zoektermen hebben ingetikt op internet (zoals een drukkookpan en een rugzak, schijnbaar mogelijke ingredienten voor een bom).

1.5 Incapabiliteit w.b. bescherming persoonlijke gegevens

Helaas is het vele malen aangetoond dat de overheid een terecht slechte reputatie heeft wat betreft het beschermen van persoonlijke gegevens. Laptops en USB sticks worden verloren, en databases gehackt. Het verzamelen van gegevens zo gevoelig als gegenereerd door een sleepnet is dan ook wachten op misbruik. Dit is echter niet alleen het geval bij overheden; talloze bedrijven worden tevens slachtoffer.

1.6 Latere misbruik data & macht

Als we voor een moment aannemen dat men de beste intenties heeft met deze maatregelen, wordt de vergaarde informatie nog altijd opgeslagen voor onbepaalde tijd. Dit maakt misbruik op een later tijdstip volledig mogelijk. Informatie kan misbruikt worden tegen politieke dissidenten en journalisten of andere burgers die de overheid niet welgevallig zijn. Machtwisselingen maken het onmogelijk om te zeggen wat er in de toekomst met de data gedaan gaat worden. Maar als de data eenmaal verzameld is, gaat deze nooit meer weg.

1.7 Metadata

Een kleine opmerking over metadata. Er wordt vaak beargumenteerd dat het afluisteren van metadata niet schadelijk is, t.o.v. het afluisteren van de inhoud van een gesprek. Echter, metadata vertelt een groot deel van het verhaal: Waar iemand is, wanneer, en met wie. Zowel in het echt (snelwegcamera's, OV chipkaart, etc), als op internet. Gecombineerd met de metadata van anderen om iemand heen is het doodsimpel om verbanden aan te leggen waar de inhoud van bv. (telefoon)gesprekken of emails niet eens voor nodig is.

2 Hoe wel verder?

Het zal altijd nodig zijn dat overheden de mogelijkheid te hebben bepaalde mensen af te luisteren met het doel bestrijding criminaliteit of terrorisme - dit

is óók een noodzaak voor het functioneren van een rechtstaat. Echter, dit moet uitsluitend mogelijk zijn bij een serieuze verdenking en bij toestemming een rechter. De voorstellen zoals ze nu staan zijn echter onacceptabel; de effectiviteit van de voorgestelde maatregelen is zéér twijfelachtig terwijl de inbreuk op de privacy van het individu groter is dan ooit tevoren.

De Westerse wereld als geheel gaat in een richting die de vrijheden van haar burgers op wijzen inperkt die doen denken aan totalitaire regimes elders in de wereld waar het Westen zich zo graag superieur aan voelt. De Nederlandse overheid zou zich actief in moeten zetten voor de privacy van haar burgers en zich niet laten beïnvloeden door buitenlandse geheime diensten. Nederland moet haar soevereiniteit serieus nemen en daarmee een voorbeeld zijn voor de rest van de wereld.

3 Slot

Dit zijn bondig mijn gedachten over dit complexe issue samengevat. Ik zou nog veel meer kunnen schrijven, maar ik wil u niet verder vermoeien met meer tekst. Als u deze discussie voort zou willen zetten, ben ik te bereiken op wesley@sesmo.eu.