Geheime surveillance bij opsporing: onafhankelijk toezicht en transparantie voor verbetering vatbaar

Wetsvoorstel hacken computers bevat onvoldoende waarborgen

In een nieuw onderzoek concluderen onderzoekers van het Instituut voor Informatierecht (IViR, Universiteit van Amsterdam) dat bij het inzetten van geheime surveillance voor de opsporing van strafbare feiten onafhankelijk toezicht en transparantie gewaarborgd moeten zijn. Uitspraken van Europese rechters hierover zijn duidelijk: er gelden dezelfde normen voor nationale veiligheid als voor de opsporing van strafbare feiten. Het rapport vertaalt deze normen in tien richtsnoeren waarmee rekening moet worden gehouden bij het ontwerp van nieuwe wetgeving.

Geheime surveillance neemt steeds verder toe. Zo bespreekt het parlement momenteel het wetsvoorstel 'Computercriminaliteit III'. Daarin zijn nieuwe bevoegdheden opgenomen om computers, mobiele telefoons en andere apparaten te 'hacken'. Door bijvoorbeeld in het geheim extra software te plaatsen kunnen gebruikers worden gevolgd en kan toegang tot de inhoud van communicatie worden verkregen. Anders dan bij gewoon aftappen, is er vaak geen medewerking nodig van de aanbieders van telecommunicatienetwerken of -diensten.

Goede waarborgen zijn nodig omdat de impact van deze wetgeving vooraf niet te overzien is. De techniek ontwikkelt zich snel en is niet voorspelbaar. Kosten vormen vaak geen barrière meer tegen grootschalige inzet.

Het rapport signaleert vier knelpunten die zich voor verbetering lenen:

- Er ontbreekt een onafhankelijke instelling die toezicht houdt op geheime surveillance. Er is geen 'systeemtoezicht': toezicht vindt voornamelijk plaats in individuele gevallen, er is slechts in beperkte mate onafhankelijk toezicht op de uitoefening in algemene zin.

- Voorafgaande toetsing van in te zetten technologieën maakt het toezicht meer compleet. Toezicht moet niet beperkt blijven tot de inzet van een middel in een concreet geval. Dit geldt in het bijzonder in het digitale domein, waar de inzet van methoden en technologieën zaak-overstijgende gevolgen kan hebben, bijvoorbeeld doordat kwetsbaarheden niet worden gedeeld en de digitale infrastructuur hierdoor zwakker blijft.

- Het toezicht moet 'daadwerkelijk en effectief' zijn. Er kan geen sprake zijn van 'rubber stamping': het voorafgaand verstrekken van lasten en toestemming moet zorgvuldig gebeuren en goed gemotiveerd worden. Er dient 'real time' toezicht te zijn, dat wil zeggen: toezicht gedurende de inzet van de bevoegdheden. Notificatieplichten moeten worden nageleefd. Betrokkenheid van deskundigen in het proces, zeker waar het gaat om de toepassing van nieuwe technologie, draagt bij aan 'tegenspraak' en tot een meer afgewogen besluitvorming.

- Er moet meer aandacht zijn voor transparantie jegens de samenleving: welke informatie wordt door de overheid verstrekt en welke gegevens mogen betrokken organisaties publiceren over verzoeken tot medewerking aan de uitoefening van bijzondere bevoegdheden.

Het rapport is bijgevoegd, dan wel te downloaden via www.ivir.nl. De auteurs van het rapport: mr. Sarah Eskens (S.J.Eskens@uva.nl, 0622774681); mr. Ot van Daalen (o.l.vandaalen@uva.nl, 0654386680) en prof. dr. Nico van Eijk (n.a.n.m.vaneijk@uva.nl, 0622409439).

Amsterdam, 22 november 2016