Nederlands Juristen Comité voor de Mensenrechten
Dutch section of the International Commission of Jurists

Tweede Kamer der Staten-Generaal
T.a.v. de vaste commissie voor Veiligheid en Justitie
cie.vj@tweedekamer.nl

Leiden, 5 december 2012

Betreft: uitbreiding opsporingsbevoegdheden op het internet

Geachte leden van de vaste commissie voor Veiligheid en Justitie,

Op 15 oktober 2012 heeft de Minister van Veiligheid en Justitie bij brief aan de Voorzitter van de Tweede Kamer der Staten-Generaal zijn voornemens kenbaar gemaakt om de opsporingsbevoegdheden van de politie op het gebied van cybercrime uit te breiden. Met deze brief vraagt het Nederlands Juristen Comité voor de Mensenrechten (NJCM) uw aandacht voor enkele kritische kanttekeningen bij dit voornemen. Het NJCM geeft u in overweging deze kanttekeningen mee te nemen bij het overleg met de Minister op 6 december a.s. over de voortgang van de nationale cyber security strategie.

Het uitbreiden van de opsporingsbevoegdheden op het internet heeft volgens de Minister tot doel het juridisch kader voor de opsporing en vervolging van cybercrime in overeenstemming te brengen met de behoeften van de opsporingsdiensten, die door de snelle ontwikkelingen in de digitale wereld vaak geen toereikende bevoegdheden hebben om cybercrime daadkrachtig te bestrijden. De Minister wil dit bereiken door onder meer het binnendringen van computers, het plaatsen van software op computers en het op afstand doorzoeken en ontoegankelijk maken van op computers opgeslagen gegevens, ook als de computer zich buiten Nederland bevindt.

Internationale afspraken
Het NJCM realiseert zich dat de in hoog tempo voortschrijdende ontwikkelingen op het gebied van ICT een aanpassing van de opsporingsbevoegdheden noodzakelijk maken. De Minister kiest ervoor om vooruitlopend op internationale afspraken de opsporingsbevoegdheden bij de bestrijding van cybercrime in Nederland uit te breiden. Door het internationale karakter van cybercrime is niet altijd duidelijk waar een computer zich bevindt en bij de opsporing is snelheid vaak geboden. De Minister wil dat in die gevallen de bevoegdheden zonder voorafgaand rechtshulpverzoek kunnen worden toegepast, ongeacht waar de computer en de gegevens zich op dat moment bevinden. Dit betekent onvermijdelijk een inbreuk op de soevereiniteit van andere landen. Als deze gang van zaken bovendien navolging zou krijgen in andere landen, zou ook de soevereiniteit van Nederland en het recht op privacy van Nederlanders geschonden kunnen worden, omdat in andere landen mogelijk een goede rechterlijke toets ontbreekt. Hoewel de Minister in zijn voorstel aangeeft dat het Cybercrimeverdrag geen bepalingen bevat die een rechtshulpverzoek noodzakelijk maken, vindt het NJCM het niet fraai om dit nationaal te reguleren en dringt er derhalve op aan dat de Minister zich vooreerst inzet om verdere internationale afspraken te maken over de te voeren procedures. Dit lijkt eens temeer aangewezen, omdat het zonder internationale samenwerking dikwijls onmogelijk zal zijn om cybercrime daadwerkelijk te vervolgen.

Daarnaast heeft het NJCM als belangrijkste inhoudelijke bezwaar bij het voorstel van de Minister, dat het op diverse punten onvoldoende uitgewerkt en gemotiveerd is. Het voorstel roept niet alleen de nodige technische vragen op, het valt ook te betwijfelen of het in huidige vorm in overeenstemming gebracht kan worden met het

Steenschuur 25
2311 ES Leiden, The Netherlands
Postal address: p.o. box 9520
2300 RA Leiden, The Netherlands
Telephone +31 (0)71 52 777 48
www.njcm.nl
ING 3540940
KvK Leiden 40445896

recht op privacy zoals onder meer neergelegd in artikel 8 van het Europees Verdrag inzake de Rechten van de Mens en Fundamentele Vrijheden (EVRM) en met de vrijheid van meningsuiting (artikel 10 EVRM).

Privacy
In het huidige digitale tijdperk staat veel persoonlijke informatie opgeslagen op PC's, tablets en smartphones. Het binnendringen, doorzoeken en vooral het ontoegankelijk maken van informatie op die geautomatiseerde werken, behelst derhalve een ernstige inbreuk op de privacy. Deze inbreuk is te vergelijken met schending van het huisrecht en zal doorgaans verder gaan dan een schending van het telefoongeheim (artikelen 12 en 13 Grondwet), onder meer aangezien hiermee toegang wordt verkregen tot een veelheid aan persoonlijke informatie. De Minister wil de eerbiediging van de persoonlijke levenssfeer waarborgen door enerzijds een voorafgaande machtiging van de rechter-commissaris verplicht te stellen en anderzijds het soort misdrijven waarvoor de bevoegdheden gebruikt mogen worden te beperken.

De aanwezigheid van rechterlijke toetsing bij de ernstige privacyschending die de inzet van deze bevoegdheden oplevert, is met het oog op de geldende jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) aangewezen. Het NJCM wijst er evenwel op dat het bij de inzet van deze bevoegdheden gaat om zeer ingewikkelde materie die de rechter-commissaris wel tot in detail moet bekijken en moet begrijpen om deze te kunnen beoordelen op noodzakelijkheid en proportionaliteit. Deze bevoegdheden kunnen op veel verschillende manieren worden ingezet, ieder met eigen consequentie voor de privacy van de betrokkene. De vraag is of een rechter-commissaris hiervoor in de praktijk voldoende tijd heeft en of op deze wijze wel effectief controle op het handelen van de politie kan worden uitgeoefend. Het gevaar voor verkeerd en te vergaand gebruik door de politie van hun bevoegdheden ligt op de loer.

Toepassingsbereik
De Minister stelt voor dat de bevoegdheden alleen kunnen worden uitgeoefend bij verdenking van strafbare feiten waarvoor voorlopige hechtenis voorzien is of waarop een maximale gevangenisstraf van vier jaar of meer is gesteld. Uit het voorstel wordt niet duidelijk of dit enkel cybercrime betreft, zoals de titel doet vermoeden, of ook andere misdrijven. Het NJCM benadrukt nogmaals de ernst van de inbreuk op de privacy van betrokkene(n), en pleit ervoor om in het wetsvoorstel een limitatieve opsomming op te nemen van de misdrijven waartegen de nieuwe bevoegdheden ingezet mogen worden.

Effect
Ten slotte zet het NJCM vraagtekens bij het daadwerkelijke effect van de voorgestelde bevoegdheden. De mogelijke technische complicaties zijn talrijk. Niet alleen kunnen cybercriminelen de ingezette bevoegdheden tegen de politie gebruiken, maar er zijn ook talloze technische bezwaren tegen het in het strafproces als bewijs laten meewegen van met deze bevoegdheden verkregen informatie. Bovendien blijven de Nederlandse opsporingsdiensten voor de daadwerkelijke vervolging van cybercrime in belangrijke mate afhankelijk van bilaterale of multilaterale samenwerking.

Gelet op het voorgaande, strekt het volgens het NJCM tot aanbeveling het voorstel van de Minister aan een kritisch onderzoek te onderwerpen.

Hoogachtend,

i/o.

Friederycke Haijer
Voorzitter NJCM