**Spreektekst GroenLinks Wet Computercriminaliteit III**

Voorzitter,

Zelfs George Orwell had dit niet kunnen bevroeden. Als hij, met kennis van de huidige technologieën, vandaag de dag 38 jaar vooruit zou blikken, wat zou hij dan schrijven? Het recent ingevoerde sociale puntensysteem in China en de illegale activiteiten van de NSA doen Orwell’s verplichte teleschermen in het huis van de Big Brother anno 2018 verbleken. Bij de voorbereidingen op de behandeling van dit wetsvoorstel dwaalden mijn gedachten soms af naar 1984. Naar de ironie dat we nu vrijwel allemaal, vrijwillig, met minimaal een veel geavanceerder telescherm rondlopen, in het wetsvoorstel ‘geautomatiseerd werk’ genoemd, dat we technisch niet begrijpen, enorm persoonlijk en belangrijk is en tegelijkertijd eenvoudig is te volgen, te spioneren en te hacken. Er is daarom een grote maatschappelijke behoefte aan een overheid die optreedt tegen criminaliteit maar tegelijkertijd de veiligheid van onze persoonlijke levenssfeer hoog in het vaandel heeft staan. En dat zij garandeert dat gebruikmaking van deze bevoegdheid altijd in overeenstemming is met de criteria zoals ontwikkeld door het EHRM en het Hof van Justitie.

Dit wetsvoorstel biedt via de hackbevoegdheid verregaande mogelijkheden om een kijkje te nemen in het dagelijks leven van mensen. Via de microfoon meeluisteren, via de webcam meekijken en dankzij de gps de locatie exact bepalen. Toetsaanslagen vastleggen, screenshots maken, gegevens vastleggen en eventueel ontoegankelijk maken, maar ook thermostaat, auto en medische apparatuur vallen onder deze wet. In feite is de hackbevoegdheid een inkijkoperatie, een heimelijke doorzoeking en afluisteren ineen. Zoals de heer Wolfsen tijdens de deskundigenbijeenkomst al zei: dichter op de huid van mensen kun je niet komen dan wanneer je in hun computers en andere apparaten kunt kijken. Het raakt daarom zelfs onze vrijheid van gedachten. Vanwege de grove inbreuk van de persoonlijke levenssfeer zal deze bevoegdheid in de ogen van mijn fractie met uiterste zorgvuldigheid worden ingezet en gecontroleerd. En juist daar bestaan nog grote zorgen over.

Mijn fractie onderschrijft de toegenomen relevantie van de aanpak van cybercriminaliteit en is het met het kabinet eens dat de opsporingsautoriteiten adequaat moeten worden toegerust om deze criminaliteit te bestrijden. Dat daar soms hacken voor nodig is, begrijpt mijn fractie ook. Maar de beperkte waarborgen in de wet, het ogenschijnlijk grote vertrouwen in de ict-kwaliteiten van onze overheid en het ontbreken van een gedegen privacy assessment maken dat onze fractie grote aarzelingen heeft bij deze wet. Bestrijding van cybercrime die het risico in zich heeft dat onze digitale samenleving onveiliger en minder beschermd wordt, schiet zijn doel voorbij. In dat licht bespreek ik hier de definitie van geautomatiseerd werk, de toetsing vooraf en achteraf, de verschillende soorten hack-bevoegdheden en de verhouding tot de meldplicht en de amvb in relatie tot de reikwijdte van het wetsvoorstel.

 Reikwijdte

Het wetsvoorstel biedt de overheid de mogelijkheid om heimelijk iemands huis binnen te dringen en er vervolgens te blijven. Digitaal, in alle apparaten die de regering maar kan verzinnen die gehackt kunnen worden, nu en in de toekomst -vandaar ook de abstracte term ‘geautomatiseerd werk’. Je kunt de techniek immers maar voor zijn. In de toekomst kan ons hele huis als geautomatiseerd werk worden beschouwd, evenals onze vervoersmiddelen. Tot dusver wil de regering niets weten van een specifieke lijst met ‘geautomatiseerd werk’. Mijn fractie vindt dat, in navolging van veel experts, een onverstandig besluit, want het maakt nogal uit welke apparatuur wordt gehackt of gebruikt, en waar die apparatuur staat. In een limitatieve opsomming kan bij de toegestane apparatuur worden ingegaan hoe , wanneer, hoe diep en waarom een bepaald apparaat is toegestaan, waarbij het opsporingsbelang, het privacybelangen en mate van indringing gezamenlijk wordt afgewogen. Heeft de regering niet op zijn minst nagedacht over specifieke criteria als toetsingskader voor de inzet en reikwijdte van inbreken van bepaalde apparatuur

Voorzitter, de ingrijpende bevoegdheden mogen volgens het wetsvoorstel alleen worden toegepast bij een verdenking van een misdrijf waarop een gevangenisstraf van acht jaar gevangenisstraf is gesteld dan wel een misdrijf dat bij algemene maatregel van bestuur is aangewezen. Deze amvb mogelijkheid maakt de inhoudelijke waarborg boterzacht. Een groot verschil met bijvoorbeeld de Duitse wetgeving dat hacken alleen is toestaat bij een acuut gevaar voor lijf en leden of wanneer de Staat gevaar loopt. Het kabinet heeft aangegeven dat het in de AMvB zal gaan over cybercrime en zedenzaken. Waar moet mijn fractie nog meer aan denken? Waarom kiest het kabinet ervoor om toekomstige beslissingen buiten het parlement om te nemen? Is hij bereid dit te heroverwegen en hiervoor een wetswijziging voor te stellen? Is immers zo’n fundamentele inbreuk in iemands persoonlijke levenssfeer, waar je figuurlijk in iemand zijn huis inbreekt en er ook blijft, zonder dat die persoon het weet, niet reden genoeg om heel precies in de wet vast te leggen wanneer dit wel en wanneer dit niet geoorloofd is? Voorzitter, op vragen over een voorhang procedure verwijst de minister naar Aanwijzing 35 van de Aanwijzingen voor de Regelgeving. Nog afgezien van het feit dat hier goede redenen zijn om parlementaire betrokkenheid wel te regelen, zou ik de minister dan ook willen wijzen op Aanwijzing 31, dat bepaalt dat in een hogere regeling niet wordt toegestaan dat daarvan bij lagere regeling wordt afgeweken. Deze aanwijzing is het gevolg van de motie Jürgens die deze Kamer ruim twaalf jaar geleden heeft aangenomen, met de strekking dat een delegatie van wetgevende bevoegdheid bij wet aan een lagere regelgever, die de lagere regelgever machtigt om af te wijken van de wet in formele zin, niet is toegelaten. In dit geval gaat het ook om de mogelijkheid van afwijking van het strikte criterium van een strafdreiging van acht jaar gevangenisstraf, en daarmee om strijdigheid met de wet. Erkent de minister dit? De heer Wolfsen van de Autoriteit Persoonsgegevens noemde het in deze Kamer *unprecedented* dat de criteria in een AMvB minder streng zijn dan die in de wet. In zijn ogen wordt de wettelijke waarborg hiermee feitelijk illusoir omdat via AMvB in theorie mogelijk wordt om de wet voor een fietsendiefstal toepasbaar te maken. Nou zal dat niet zo snel gebeuren, maar als we kijken naar de praktijken die de Volkskrant zaterdag onthulde bij een vermoeden van bijstandsfraude? Wie garandeert ons dat het daar op termijn niet op zal uitdraaien? Een lagere regelgever heeft niet de bevoegdheid om van een regeling van een hogere regelgever af te wijken, tenzij de hogere regelgever de lagere daartoe bevoegd verklaart. Met de term afwijken wordt gedoeld op de situatie dat de lagere regelgeving bepalingen bevat die niet slechts uitwerking of invulling inhouden van formeelwettelijke bepalingen, maar daarmee als het ware ‘strijdig’ zijn. Ook al is een dergelijke constructie strikt genomen geoorloofd, zij leidt tot onoverzichtelijke regelgeving en dient derhalve in beginsel niet te worden toegepast.

De regering gaf aan dat, ik citeer, kan worden verwacht dat de inzet van onderzoek in een geautomatiseerd werk mogelijk ook andere vormen van politie-inzet kan vervangen. Hoe ziet de regering dit? Wat voor andere vormen? En hoe beziet zij dit in het licht van de proportionaliteits- en subsidariteitstoets?

Toetsing

Voorzitter, onze fractie vindt het cruciaal dat de vergaande hackbevoegdheid is omkleed met onafhankelijk en bindend toezicht in elk stadium. Het wetsvoorstel voorziet in een toetsing vooraf door de Centrale Toetsingscommissie van het OM en de rechter commissaris. De een zal meer beleidsmatig zijn en de andere individueel, ze vullen elkaar dus goed aan. Wel zouden de leden bevestigd willen horen dat het verzoek om toestemming aan de RC in een individueel geval vergezeld van een motivering ten aanzien van de gekozen apparatuur, en niet alleen op de inzet van de bevoegdheid in het algemeen? Dat lijkt onze fractie voor een goede proportionaliteitstoets van belang. Ook heeft mijn fractie vragen naar de benodigde expertise van de rechter commissaris. Wordt er gedacht aan gespecialiseerde RC’s, of wordt anderszins geïnvesteerd in up-to-date kennis? De toets achteraf is echter beperkter, omdat die is belegd bij de inspectie van J&V. In de ogen van mijn fractie ziet deze niet op de rechtmatigheid van de inzet van het hacken, is dat juist en zo ja, waarom acht de minister deze toets voldoende? Volgens de minister opereert de inspectie onafhankelijk binnen het ministerie maar erkent hij dat de inspectie als onderdeel van het minister niettemin een ander soort onafhankelijkheid heeft dan een orgaan dat op afstand staat? Ook ontbreekt het de inspectie aan cruciale bevoegdheden zoals het onder ede horen van ambtenaren. Het toezicht achteraf schiet in onze ogen daarom te kort. Temeer omdat lang niet alle zaken voor een zittingsrechter zullen komen en dus niet achteraf aan een rechterlijke toets worden onderworpen.

Dit geldt ook, en wellicht des te meer bij de inzet van de hackbevoegdheid met handhavingsdoeleinden, bijvoorbeeld bij het ontoegankelijk maken van online-informatie of het onklaar maken van botnetinfrastructuur. Ook hier zou toezicht achteraf gegarandeerd moeten zijn. Erkent de minister het belang hiervan, en welke mogelijkheden ziet hij om dit te versterken. Is ook overwogen om het toetsingsmodel van de CTIVD ook hier toe te passen, waar de inzet achteraf op een integrale en beleidsmatige wijze kan worden beoordeeld?

De toetsing achteraf bij verstoringsacties wordt sowieso bemoeilijkt omdat verslaglegging van een hack ontbreekt. Daarnaast vindt er controle op de daadwerkelijke hacks plaats via logging. Acht de minister dit afdoende? Ook hier hanteert de overheid eenzelfde constructie met de AMvB’s als bij de hackbevoegdheid. Waarom hier niet een lijst aanleggen van materiaal dat allemaal in aanmerking komt voor eventuele blokkade? Ook hier zijn wettelijke waarborgen van groot belang, omdat deze bevoegdheid immers ook raakt aan de vrijheid van meningsuiting en vrije nieuwsgaring. Hoe gaat de minister voorkomen dat een te ruim gebruik van deze bevoegdheid de weg openzet naar een censurerende internetpolitie?

Voorzitter, er geldt een notificatieplicht zodra belang van het onderzoek dat toelaat, een criterium dat voor velerlei uitleg vatbaar is. Kan de minister nader toelichten hoe hier in de praktijk doorgaans mee wordt omgegaan? En wordt er altijd genotificeerd als er wordt afgezien van verdere opsporing en vervolging? Ook blijft notificatie achterwege als uitreiking van de mededeling redelijkerwijs niet mogelijk is. Ook hier de vraag naar de toepassing en welke inspanningen worden verricht om notificatie te realiseren. Is het juist dat een sanctie ontbreekt bij niet nakomen en zo ja, wat is hiervan de reden? Is het niet van cruciaal belang dat een betrokken burger geïnformeerd wordt en daarmee ook de mogelijkheid krijgt om zich hiertegen teweer te stellen? En hoe zit het met de rechtpositie van de burger? Hoe kan die zich wapenen tegen onterechte verdenkingen? De Nationale Ombudsman is in onze ogen onvoldoende. Zou niet net als bij de WIV een extra proportionaliteitstoets nodig en hoe om te gaat nevenschade?

Ook maken wij ons zorgen over de positie van journalisten. Afgelopen week werd nog duidelijk dat het OM de belgegevens van een journalist heeft opgevraagd, gekregen en uiteindelijk een poging ondernomen om hem af te luisteren. Hoe ziet de minister dit? Is het in dit kader niet zeer wenselijk om over voorliggend wetsvoorstel pas te stemmen als het wetsvoorstel over bronbescherming in strafzaken is behandeld, of in elk geval om beide wetten gelijktijdig inwerking te laten treden? Graag een reactie.

Voorzitter, als Nederlandse diensten over de grens gaan hacken zonder instemming van de betreffende autoriteiten, maken zij een inbreuk op de soevereiniteit van dat land. De regering heeft aangegeven dat er goede werkafspraken zijn met Europese landen en er altijd een rechtshulpverzoek wordt ingediend door Nederland in het land waar men wil hacken. Behalve blijkbaar, aldus staatssecretaris Dijkhoff bij de behandeling in de Tweede Kamer, bij landen die bekende vrijplaatsen zijn voor criminelen. ‘Dan ga je niet zitten wachten op een rechtshulpverzoek’, zei hij losjes. Deelt deze minister de opvatting van zijn voorganger? En zo ja, welke rechtvaardiging ligt er ten grondslag aan deze schending van het internationaal recht? Op welke landen doelt het kabinet en wat zijn de criteria om af te zien van een rechtshulpverzoek? Heeft de regering nagedacht over de gevolgen van repercussies? En vormt het niet doen van een rechtshulpverzoek ook een onderdeel van de toets door de rechter commissaris?

De overheid en ICT – kwetsbaarheden

Er is al veel gezegd over kwetsbaarheden en het WanneCry-incident is een mooi voorbeeld van hoe het niet rapporteren van een kwetsbaarheid juist heeft geleid tot een mondiale cyberaanval. Voor mijn fractie is het simpel: op de zwarte markt spyware kopen en deze software hoog in de servers van de providers installeren met het risico dat de overheid het systeem onveiliger maakt, gaat te ver. Klopt het dat Nederlandse politieagenten FinFisher-spyware hebben gebruikt, of nog steeds gebruiken? Zo ja, bent u ervan op de hoogte dat het niet gereguleerd is en dat het voor fundamentele kwetsbaarheden kan zorgen in de systemen van de providers? Onze fractie vindt het onwenselijk dat onbekende kwetsbaarheden die met hacksoftware worden gebruikt, niet worden gemeld. De meldingsplicht wordt zo door het gebruik van deze software een dode letter. Erkent de minister dat en zo ja, hoe gaat hij voorkomen dat opsporingstechnieken tot meer onveiligheid leiden? Is de minister van plan om met beleid te komen met een helder toetsingskader voor de afweging tussen enerzijds het achterhouden van kwetsbaarheden uit opsporingsbelang en anderzijds het algemene belang van zo snel mogelijk melden? Zolang dat niet aanwezig is lijkt ons de regering zich verre zou moeten houden van het inkopen en gebruiken van ongereguleerde spyware.

Gebruikmaken van bestaande kwetsbaarheden en die pas later melden, is van een andere orde. Maar ook hiervoor geldt wat ons betreft dat de opsporingsdiensten deze zo snel mogelijk melden.

Voorzitter, we kunnen simpelweg niet vooraf weten op welke schaal en met welke gevolgen het hacken in de toekomst wordt ingezet. Bij de evaluatie zal een goed inzicht moeten zijn in de wijze waarop de bevoegdheden zijn gebruikt en welk effect het heeft gehad. Het lijkt onze fractie van belang om tot de evaluatieperiode alle hackacties achteraf laten toetsen en daarin specifiek meenemen in hoeverre de schending van de persoonlijke levenssfeer gerechtvaardigd was. Hoe kijkt de minister hier tegenaan? Aan de hand van welke criteria zal de minister de wet gaan toetsen?

Tot slot

Voorzitter, we leven in een tijd waar de privacy van de mensen steeds meer onder druk staat. Soms komt dat door onszelf als wij vrijwillig onze data afstaan, soms omdat we te pas en te onpas worden gevraagd akkoord te gaan met gebruikersvoorwaarden en cookies en soms komt dat door een overheid die steeds dieper in het leven van haar burgers kan doordringen. De analyse van de gevolgen van de incrementele aantasting van onze persoonlijke levenssfeer door digitalisering zijn pas achteraf te maken. Privacy is meer dan veiligheid. Toezicht op wat we denken, lezen, bekijken, schrijven, bespreken, kan ons verlammen in het verkennen van nieuwe ideeën en in het uiten van onze identiteit. Ook is een gezond wantrouwen naar de overheid van belang voor de bescherming van onze grondrechten. Naar de ultieme effecten van een te indringend toezicht hoeven we niet alleen te gissen. In China zorgt het puntensysteem nu al ervoor dat iemand de trein niet meer kan nemen als hij zijn moeder niet vaak genoeg bezoekt. Technologie is niet neutraal en tevens stuurbaar. Dat lijkt dit kabinet ook te beseffen, maar helaas meer ten faveure van de opsporingsmogelijkheden dan van onze persoonlijke levenssfeer. Net als bij de Wiv ligt er in de basis een redelijk goede wet, maar de ruime criteria en uitzonderingsmogelijkheden en het beperkte toezicht achteraf zijn voor ons toch reden tot zorg. Wij kijken uit naar een reactie van de minister.