PRIVACY INTERNATIONAL

Privacy International
62 Britton Street
Clerkenwell EC1M 5UY
United Kingdom

Uploaded at: https://www.internetconsultatie.nl/wiv/reageren/1

27 August 2015

Dear Sir/Madam,

RE: SUBMISSION TO THE INQUIRY INTO THE DRAFT LAW ON INTELLIGENCE AND SECURITY SERVICES 2015

We make this submission on behalf of the British human rights organisation Privacy International.

Privacy International was founded in 1990, and is the leading non-governmental organisation promoting the right to privacy across the world. It focuses, in particular, on tackling the unlawful use of surveillance. It is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Council of Europe, the European Parliament, the Organisation of Economic Co-operation and Development and the United Nations.

Privacy International is actively engaged in scrutinising and critiquing surveillance and signals intelligence laws and policies across the globe. In particular, we are highly active in the ongoing surveillance reform debate in the United Kingdom, where the government will soon seek to enact legislation that will replace all surveillance laws currently in force in Britain. Our internal expertise on surveillance laws and policies is unsurpassed in Britain, where ware also the leading organisation challenging unlawful surveillance practices in British courts.

We wish to express a number of concerns about provisions currently contained in the Draft Law on Intelligence and Security Services 2015 ("the Draft Law"). In particular, the provisions relating to bulk interception, the lack of judicial authorisation, the breaking of encryption, and the hacking of computers and devices raise serious concerns when considering he law's compliance with internationally-agreed human rights norms. We urge the Dutch government to refrain from expanding the Netherland's surveillance powers beyond what is necessary and proportionate in a democratic society. If enacted, not only would this Law make the Netherlands a country with some of the broadest and most intrusive surveillance systems in the world, but it would set a worrying example for countries which don't enjoy your strong democratic

tradition and rule of law.

Below we have set out some of our concerns with the legislation.

Bulk interception powers

We understand that current Dutch law allows for the bulk (i.e. non-specific or non-targeted) interception of ether-bound, but not cable bound, communications where they have a foreign source or destination, for the purpose of signals intelligence ("SIGINT") search. SIGINT selection could be undertaken on any ether-bound communications. However, given that the percentage of domestic communications likely to travel by the ether is negligible, these powers ostensibly allowed only for the bulk interception and analsyis of foreign communications, and even then only ether-bound communications, which in the digital era remains a small percentage of civilian communications. In short, the currently law constrains the ability of the intelligence and security services to do mass surveillance on ordinary individuals' communications, whether they be in the Netherlands or abroad.

The proposed changes will alter this situation severely, essentially introducing a mass surveillance capability into Dutch law. The provisions in the Draft Law relating to non-specific interception do not restrict the exercise of such powers to foreign communication, nor – more importantly – do they restrict interception to ether-bound communications. The result is that the Draft Law authorises the intelligence and security services to conduct mass surveillance of cable bound communications – the cables that carry the private and intimate communications of millions of ordinary people.

The fact that the Draft Law introduces numerous checks and authorisations stages, and requires the interception to be "purpose-oriented" (doelgerichtheid) does not change that the Draft Law will authorise the interception of millions of communications under broad justifications. The Draft Law does not restrict how broad the purpose can be, nor does it restrict how many communications can be intercepted at any one time for the achievement of that purpose. In that context, and assuming that a purpose as broad as "countering terrorism" would be sufficient under the Draft Law (there being no contraindication expressed), the Draft Law does not restrain the intelligence and security services from intercepting all of the communications in the Netherlands all of the time. Furthermore, the Draft Law proposes to extend the retention period for raw intercepts from one year to three, and enables the Dutch intelligence and security services to share raw bulk intercepts (metadata and content) with foreign intelligence and security services.

The interception of communications constitutes an interference with the right to privacy of those communications under Article 8(1), whether made via email, phone, text message, or social media: see e.g. Klass v Germany, 6 September 1978, Series A No 28 at §41; Weber and Saravia v Germany, ECHR 2006 XI at §77; Kennedy v United Kingdom 26839/05 18 May 2010 at §118. The same is true in respect of accessing communications data or 'metadata': see e.g. Malone v United Kingdom 2 Aug 1984, Series A No 82 at §84. Further interferences arise from the collection and retention of such material (see e.g. Amann v Switzerland [GC] ECHR 2000-II – especially on a searchable database – and its transmission to other authorities (Weber and Saravia v Germany at §79)).

The European Court of Human Rights has made no distinction as to the severity of the interception effect when the interception is effected by an automated system or computer. Indeed, the Court has also found that the interception and/or storage of a communication constitutes the interference, and that the subsequent use of the stored information has no bearing on that finding. In Amman v Switzerland (2000) the ECtHR followed its judgment in Leander v Sweden (1987) that "[b]oth the storing and the release of [secret police-register information], which were coupled with a refusal to allow Mr. Leander an opportunity to refute it, amounted to an interference with his right to respect for private life...".

Equally, the Court has found that it does not matter whether the information gathered on an individual was sensitive nor whether the applicant had been inconvenienced in any way. In Amman the Swiss government submitted that the establishment of a database of surveillance- derived information was not an interference with the right to privacy because it "contained no sensitive information about the applicant's private life". The Court held (at [70]): "[i]t is sufficient for it to find that data relating to the private life of an individual were stored by a public authority to conclude that... the creation and storing of the impugned card amounted to an interference, within the meaning of Article 8, with the applicant's right to respect for his private life."

In Liberty and Others v United Kingdom the ECtHR reiterated that the mere existence of powers "permitting the examination, use and storage of intercepted communications constituted an interference with the Article 8 rights of the applicants" (at [57]). This sentiment has been echoed by the United Nations High Commissioner of Human Rights who, in her report on the right to privacy in the digital age, noted that "[t]he very existence of a mass surveillance programme thus creates an interference with privacy. The onus would be on the State to demonstrate that such interference is neither arbitrary nor unlawful."

The Draft Law thus contains a number of provisions which do not comport with international human rights standards. Mass surveillance systems than enable the blanket interception of cable-bound communications, even if for short periods of time, can not be judged to be proportionate. It can never been necessary in a democratic society to place an entire population's communications under the watchful eyes of security services, no matter what ends are served. Moreover, when intercepted communications are shared with foreign intelligence services, not only is a further interference with privacy rights occasioned, but the risk that such data will be subsequent used in a way that further imperils the rights of individuals is increased significantly.

Recommendations:

- **Prohibit the bulk interception of cable-bound communications**
- **Ensure that the Draft Law provides that the interception of communications and acquisition of communications data can only take place on a targeted basis where necessary and proportionate. To this end, ensure the interception powers in the Draft Law meet the standards articulated in the International Principles on the Application of Human Rights to Communications Surveillance (at www.necessaryandproportionate.org)**
- **Ensure that the Draft Law provides equal human rights protections for both**

Dutch citizens and foreigners

Lack of judicial authorisation

It is of serious concern that the Draft Law does not include any role for judicial authorisation, ex ante or ex post. At no stage of the interception process – from collection, to processing, to analysis – is an independent judicial authority consulted for authorisation or review.

If enacted, this element of the Draft Law would make the Netherlands an outlier in terms of best international practice. In order for interferences with the right to privacy, in the form of secret surveillance measures, to be in compliance with Article 8, they must be "in accordance with the law". As explained n Malone v United, the phrase "in accordance with the law" does not merely refer back to the presence of domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention (at [67]).

In Klass, the Court emphasised that "[t]he rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure" (at [55]). Although the Court in Klass agreed that "it is in principle desirable to entrust supervisory control to a judge," it did not go so far as to hold that prior judicial authorisation was required in every case so long as the relevant authorising body was "sufficiently independent" of "the authorities carrying out the surveillance" to "give an objective ruling" and was also vested "with sufficient powers and competence to exercise an effective and continuous control" (at [56]).

There is a growing recognition by courts in Europe and around the world that judicial control of surveillance is the most appropriate and effective safeguard against abuse and guarantor of the lawfulness of surveillance measures. The most recent and pertinent decision comes from the Court of Justice of the European Union ("CJEU") in its decision of Digital Rights Ireland v Minister for Communications & Ors. That case concerned the compatibility of Directive 2006/24/EC of the European Parliament on the retention of communications data, with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ("the Charter") and Article 8 of the Convention. The mandatory blanket retention of data by communications service providers is a surveillance measure justified on the grounds that it is a necessary and effective investigative tool for law enforcement and the protection of national security. The CJEU described the directive as a causing a "wide-ranging" and "particularly serious" interference with the rights to privacy and data protection enshrined in Articles 7 and 8 of the Charter. In questioning the necessity of the measures mandated by the directive, the Court noted, inter alia (at [62]):

> "In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the

data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits."

Beyond Europe, courts in Canada and the United States have recently issued decisions affirming that surveillance measures, including access to data retained by communications service providers, must be subject to judicial control or dependent upon the issuance of a judicial warrant. In the case of R v Spencer, the Supreme Court of Canada considered whether police obtaining identity information from an Internet Service Provider (ISP) without prior judicial authorisation, which information was subsequently used to convict an accused of possession of child pornography, was in compliance with the Canadian Charter of Rights. The Court considered that a request from police that an ISP voluntarily disclose identity information amounts to a search. Given that "[a] warrantless search, such as the one that occurred in this case, is presumptively unreasonable" the Crown had to rebut the presumption by establishing that the search was authorised by law, and carried out in a reasonable manner. The Court found that there was no lawful authority for the police's search, and thus it was unlawful.

The US case of Riley v California concerned the search of digital information on a cell phone. The Supreme Court of the United States considered whether police were required by the Fourth Amendment to the US Constitution, which pertains to search and seizure, to obtain a judicial warrant prior to conducting such a search. In a unanimous decision, the Court held that the police generally may not search digital information on a cell phone seized from an individual who has been arrested without first obtaining a judicial warrant.

Recommendations:

- **Provide for ex ante judicial authorisation of interception of communications and acquisition of communications data**
- **Provide for ex post judicial review of surveillance measures**

Powers to break encryption

We are very concerned about Article 33 of the Draft Law, which appears to authorise the intelligence and security services to break or undermine encryption of telecommunications or data, coupled with Article 30-5 to 30-8, which contain the power to compel anyone to assist in the decryption of data by handing over keys or providing decrypted data.

Any attempts to undermine the free use of encryption in digital communications could have serious impacts on the ability of individuals to enjoy their human rights. Encryption is used by every single person who uses a cell phone or a computer, and it protects their personal details and communications from interference by cyber criminals, identity thieves, hackers, and States. The use of encryption is the only way to ensure digital communications – ranging from online financial transactions to cell phone calls to emails – are protected from interference.

By granting the intelligence and security services the power to break encryption, or demand the disclosure of encryption keys, the Draft Law seriously undermines the essential role that encryption plays in modern digital communications. The existence of such a power prevents individuals from being able to reliably communicate knowing that their correspondence is free from interference, and thus has a severe chilling effect on the exercise of free expression. The ramification of such provisions will be felt far beyond the Netherlands: because of the way that digital communications flow across borders and around the world, the existence of targeted powers to remove or defeat encryption in one State has implications for all individuals, and creates a chilling effect for people around the world that is far greater than the sum of isolated instances in which such powers might be deployed.

Furthermore, decryption orders require a delicate assessment of the balance between different human rights (e.g. right to privacy, right to freedom of expression anonymously) and legitimate interests. Such assessment should be made by impartial and independent judicial authorities to effectively guarantee the respect and protection of the right to privacy. This is particularly so in light of the fact that failure to comply with such orders is often considered a criminal offence. Unfortunately, the Draft Law contains no such requirement that a decryption order be judicially authorised.

Recommendations

- **Remove provisions in the Draft Law enabling the security services to break encryption and compel the disclosure of encryption keys**
- **With respect to decryption orders, ensure that the use of such powers is subject to ex ante judicial authorisation**

Expansion of hacking/computer network exploitation powers

Hacking, also known as computer network exploitation (CNE), is an extremely intrusive form of surveillance. It can yield information sufficient to build a total profile of a person, from his daily movements to his most intimate thoughts.

The Netherlands is one of the only countries in the world with legislation permitting its intelligence and security services to use CNE as a form of surveillance. This is because, in most States, hacking is seen as a hugely invasive form of surveillance that may not, in fact, be acceptable in a democratic society. In this context, the provisions in the Draft Law which purport to expand the powers of the services to hack are extremely worrying, both in the sense that they expand already concerning powers, as for the potentially detrimental example they set to other States.

We urge the Dutch government to proceed with caution when expanding the services hacking powers, particularly – as is proposed in Article 30 – introducing greater powers to use CNE for reconnaissance and against third parties.

Such powers are not only extremely intrusive, they also have the potential to undermine the security of the target device and the internet as a whole. Fundamentally, malware and other CNE methods are designed to allow an unauthorised person to control another's computer. The security hole created can be exploited by anyone with the

relevant technical expertise. Passwords, encryption keys and personal files can be collected and copied, either to further other intelligence aims or for a criminal purpose, depending on who has found the vulnerability in the target's system. CNE is the modern equivalent of breaking into a residence, and leaving the locks broken or damaged afterwards.

Furthermore, computer systems are complex and unpredictable. And malware is often not fully vetted to determine its effects on the system.[1] Its installation alone may cause damage, such as the destruction of property or data on the computer, including draft documents or family photos. Intentional alteration is also possible, raising serious concerns regarding the integrity of evidence obtained from the target device. Covert modifications of the system and the planting of data and network logs could lead to misrepresentations of activity and perversions of justice.

The integrity of every network, including the entire internet, is at issue. When the intelligence services release malware, they rarely will be able fully to control its distribution. For instance, the malware the US government used to infect Iranian nuclear facilities, Stuxnet, was later found on computers at the corporation Chevron. [2]If a watering hole is deployed, the government cannot dictate who lands on the infected website. A link to a fake news story, directly emailed to a target, might be forwarded on to others or posted on social media. A server that is the subject of a man in the middle attack could host multiple websites, exposing all those website users to exploitation. If a network communications hub is targeted, that security vulnerability will expose all network users. Or the attack might shut down the network entirely, such as occurred when the US attacked communications infrastructure in Syria.[3] Accordingly, CNE may lead to significant economic losses for network administrators and users and create backdoors for outside access to all personal information contained within the network.

Whether CNE is ever justifiably deployed, therefore, is still an open question. It is very difficult to balance the desire for a new, very powerful surveillance tool with the likelihood of sabotaging the security of our business and personal communications. The privacy intrusion involved further complicates the matter, as CNE reaches further into our lives and thoughts than any heretofore known form of surveillance.

For these reasons, Privacy International urges the Dutch government to very seriously consider if CNE can ever be safely and proportionately used. As the UN Special Rapporteur on freedom of expression has declared, "[f]rom a human rights perspective, the use of such technologies is extremely disturbing."[4]

---

1 Chaos Computer Club, "Chaos Computer Club analyzes government malware" (October 8, 2011), available at: https://www.ccc.de/en/updates/2011/staatstrojaner

2 Rachel King, "Stuxnet Infected Chevron's IT Network," *Wall St. J.* (8 November 2012), available at http://blogs.wsj.com/cio/2012/11/08/stuxnet- infected-chevrons-it-network/.

3 Spencer Ackerman, "Snowden: NSA accidentally caused Syria's Internet blackout in 2012," *The Guardian* (August 13, 2014), available at: http://www.theguardian.com/world/2014/aug/13/snowden-nsa-syria- internet- outage-civil-war

4 *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, UN General Assembly, A/HRC/23/40, at paragraph 62, available at

Recommendations

- **Assess whether CNE can be used at all in a manner that is necessary and proportionate.**
- **If the CNE power is to be retained, it should only be deployed in the most compelling and narrowly-defined circumstances, with the greatest oversight and safeguards. The following set of principles, if adopted, would help ensure that CNE is used only infrequently when most needed and justified.**
  1. **A CNE operation shall not be undertaken unless there is a high degree of probability that a serious crime or specific threat to national security has been or will be carried out;**
  2. **A warrant for CNE shall not issue unless there is a high degree of probability that evidence relevant and material to a serious crime or specific threat to national security would be obtained by accessing the equipment identified;**
  3. **Any information accessed via CNE shall be confined to that which is relevant and material to the serious crime or specific threat to national security alleged;**
  4. **Before a warrant for CNE is issued, the applicant must demonstrate that other less invasive techniques have been exhausted or would be futile, such that CNE is the least invasive option;**
  5. **The intelligence and security services should not engage in CNE that is likely to make the device targeted, or communications systems generally, less secure;**
  6. **The use of CNE should be subject to the highest levels of judicial authorisation;**
  7. **CNE should be subject to stringent independent oversight;**
  8. **CNE should not be used to circumvent other legal mechanisms for obtaining information;**
  9. **Any information obtained via CNE should be accessed only by authorised intelligence and security agencies, and used only for the purpose and duration for which authorisation was given; and**
  10. **Any individual or entity that has been a target of CNE should be able to seek redress, including those from other countries who may have been targeted.**

---

http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

Reactie op consultatie wetsvoorstel inlichtingen- en veiligheidsdiensten

30 augustus 2015

Geachte heer, mevrouw,

Dank voor de mogelijkheid om een reactie te geven over de herziening van de Wet op de inlichtingen- en veiligheidsdiensten 2002. De belangrijkste wijziging in het wetsvoorstel van het kabinet is om de AIVD en MIVD de bevoegdheid te geven grootschalig het internet af te luisteren. Dat is een aantoonbaar ineffectieve en contraproductieve maatregel waarvoor elke noodzaak, verantwoording en onderbouwing ontbreekt.

Wij onderschrijven het belang van een goede inlichtingen- en veiligheidsdienst. Daarom moet er verder gekeken worden dan naar uitbreiding van bevoegdheden. Er zal veel capaciteit verloren gaan aan het verzamelen en doorspitten van een grote berg nieuwe gegevens van onverdachte burgers. Telkens weer blijken daders van aanslagen al bij instanties bekend te zijn. De grootste risico's komen ook af van de groep die al bekend is. De AIVD mag deze personen en organisaties op internet al lang afluisteren. Het is niet effectief, niet noodzakelijk en daarmee ook niet proportioneel onverdachte burgers af te luisteren als verdachten al op een andere manier in beeld zijn. Het tast de grondrechten van burgers onnodig aan.

Onze aanbeveling is om daarom te stoppen met de uitwerking van dit wetsvoorstel. In onderstaande acht punten treft u in detail onze aanbevelingen over de herziening van de wet op de inlichtingen- en veiligheidsdiensten uit 2002 aan.

Inhoudsopgave

1. Laat de AIVD vooral de burger beschermen tegen nieuwe dreigingen

In de evaluatie over de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002) door de commissie Dessens wordt een antwoord gezocht op toenemende terroristische dreiging. De commissie spreekt daarbij over 'staatsveiligheid' en 'nationale veiligheid'. De wereld is echter drastisch veranderd. Niet de staat, maar de individuele burger wordt als eerste bedreigd door terrorisme. De aanslagen in Parijs met 17 doden zijn met name een gevaar voor de burgers gebleken en veel minder voor de Franse staat. Waar we voorheen vreesden om door een andere mogendheid geannexeerd te worden, is het nu vooral de individuele burger die het slachtoffer kan worden van onder andere internetcriminaliteit, 'lone wolves' en terrorisme. In de herziening van de Wiv 2002 moet daarom niet alleen vanuit nationale veiligheid maar ook vanuit veiligheid voor burgers worden gedacht. Vanuit het perspectief van de individuele veiligheid zal blijken dat er andere maatregelen nodig zijn om de nieuwe dreigingen het hoofd te bieden. In dit licht is bijvoorbeeld versleuteling van communicatie door burgers toe te juichen, terwijl dat vanuit nationale veiligheid gezien niet het geval zal zijn. Voor de burger is privacy ook veiligheid.

Burgers meer ondersteunen

De commissie Dessens concludeert terecht dat er steeds meer communicatie over internet plaatsvindt, dat mensen daar noodgedwongen steeds afhankelijker van worden, maar dat men daarmee ook kwetsbaarder wordt. (blz. 72) Burgers worden gestimuleerd om gevoelige gegevens te delen door gebruik te maken van bijvoorbeeld de slimme meter, het Elektronisch PatiëntenDossier (EPD/LSP) en internetbankieren. Steeds meer overheidsdiensten zijn alleen via DigiD bereikbaar. Een inbreuk op die communicatie betekent een veel grotere inbreuk op de persoonlijke levenssfeer dan dat bij de invoering van de Wiv 2002 betekende.

Volgens de commissie voelen burgers steeds sterker de noodzaak zich te beschermen tegen ongewenste toegang van hun persoonsgegevens. Tegelijkertijd stelt de commissie dat het voor de overheid moeilijker wordt om de veiligheid te garanderen. De AIVD dient daarom te helpen individuele burgers beter in staat te stellen zichzelf te beschermen op het internet. Zo moeten kwetsbaarheden in systemen die de AIVD ontdekt, terstond worden gemeld.

Ook in een onderzoek (pdf) van de Raad van Europa van 26 januari 2015 wordt nadrukkelijk verwezen naar de zelfbescherming door burgers. (punt 124, blz. 32) Het onderzoek concludeert dat versleuteling van communicatie de laatste verdedigingslijn is tegen misbruik van gegevens. Zoals de politie in de reële wereld mensen wijst op het belang van goed hang- en sluitwerk, zo zou de AIVD in samenwerking met het Team High Tech Crime van de politie een (ondersteunende) taak moeten hebben om mensen voor te lichten zichzelf door middel van encryptie te beschermen. Dit alles in plaats van de huidige voorgestelde verruiming van inbreuken op gegevens van onverdachte burgers door onder andere de AIVD.

2. Verbied ongericht aftappen van (bulk-)communicatie

Het belangrijkste element in het wetsvoorstel is om op het internet grootschalig informatie van voornamelijk onverdachte burgers af te luisteren en op te slaan. Maar nergens wordt de noodzaak daarvan onderbouwd.

a. In het rapport van de commissie Dessens wordt als enige onderbouwing gegeven dat afnemers hier behoefte aan hebben. *"Volgens diverse belanghebbenden vragen voortschrijdende technologische ontwikkelingen om een aanpassing van de huidige bevoegdheden om te kunnen blijven inspelen op de dreigingen die afkomen op de Nederlandse samenleving."* (blz. 74). Het is een open deur van formaat dat afnemers van informatie liever meer informatie willen hebben. Zeker als zij de rekening er niet voor betalen. Dergelijke vage uitspraken tonen op geen enkele wijze de noodzaak aan van deze vergaande inbreuk op grondrechten van burgers.
b. Ook minister Plasterk blijkt desgevraagd in de Eerste Kamer niet aan te kunnen geven hoe het ongericht verzamelen van gegevens daadwerkelijk bijdraagt aan het voorkomen van aanslagen of andere zaken. Op de vraag van Kamerlid Gerkens (SP) hoe doelmatig ongerichte interceptie is, antwoordt de minister: *"Ik vind het dus moeilijk om daar een antwoord op te geven."* Ook op de vraag van Kamerlid Duthler (VVD) over de doelmatigheid en de doeltreffendheid, antwoordt Plasterk dat dat vooraf niet is vast te stellen. *"Of het uiteindelijk effectief zal zijn, weet je natuurlijk op dat moment niet."* In zijn voorstel zelf komt Plasterk niet verder dan *"Om zicht te houden op deze dreigingen zijn de diensten afhankelijk van een adequate toegang tot telecommunicatie. [..] Bijzondere bevoegdheden [..] zijn daarbij onmisbaar."* (blz. 2)
c. Ook de toezichthouder CTIVD stelt in haar jaarverslag 2014-2015 dat de noodzaak voor het verruimen van afluisterbevoegdheden **niet is onderbouwd**.
d. De Eerste Kamer heeft een **duidelijke motie** aangenomen dat van een sleepnet om ongericht informatie te verzamelen geen sprake kan zijn. De motie is door een **brede meerderheid** van PvdA, het CDA, de ChristenUnie, GroenLinks, SP, D66, 50PLUS, PvdD en de OSF aangenomen.
e. De bewaarplicht van telecomgegevens ging beduidend minder ver. Er werd minder bewaard en de periode dat gegevens bewaard werden was vele malen korter. Zowel de Europese rechter als de Nederlandse rechter hebben **deze wet verboden** omdat het onevenredig inbreuk maakte op de privacy van onschuldige burgers.
f. Ongerichte massa-surveillance is altijd in strijd met de fundamentele rechten van mensen. Dit is duidelijk gemaakt door het Europese Hof dat in 2014 het massaal opslaan van telecomgegevens van burgers heeft **verboden**. De Raad van State **onderschrijft** dit oordeel en stelt dat ook de massale registratie van auto's op snelwegen door kentekenscanners illegaal zou zijn.
g. De AIVD beschikt al over de mogelijkheid van een sleepnet, zij het zeer beperkt. De AIVD kan een organisatie als verdacht aanmerken en de personen binnen die organisatie afluisteren. Ook op internet. De criteria voor wat een organisatie is, zijn niet erg duidelijk. Door ruime criteria te kiezen, ontstaat al een beperkt sleepnet, maar dan toch weer gericht rond een verdachte organisatie. De AIVD hanteert deze werkwijze al. Dit lijkt een logischere keuze dan een vrijwel onbeperkt sleepnet.
h. In het eerder aangehaalde **onderzoek** van de Raad van Europa wordt onomwonden geconcludeerd dat *"massasurveillance geen effectief middel is in de strijd tegen terrorisme of georganiseerde misdaad in vergelijking met traditionele, gerichte surveillance"*. (punt 126, blz. 32). Ook erkende terrorisme-experts als **Beatrice de Graaf en Ben Hayes** concluderen dat ongericht massaal burgers afluisteren niet effectief is.
i. Daders van aanslagen blijken in vrijwel alle gevallen al bekend te zijn bij 'de instanties'. Dat bleek ook bij weer de aanslag in Parijs op Charlie Hebdo, de verijdelde aanslag op de Thalys en de aanslag in de joodse wijk in Brussel. Er is geen onderzoek bekend, waaruit blijkt dat een ongericht sleepnet daders in het vizier bracht en een aanslag zou hebben voorkomen. Het is zinvoller om te onderzoeken

waardoor informatie niet op de juiste plek terecht komt of waardoor verkeerde beslissingen worden genomen.

j. De NSA verzamelt op grote schaal ongericht informatie. Ook de NSA heeft niet aan kunnen tonen dat er aanslagen door zijn voorkomen. De mededeling van de directeur van de NSA dat er 54 aanslagen zouden zijn verijdeld, bleek een leugen tegenover het Amerikaanse congres.

3. Sta niet toe dat de AIVD een geheime DNA databank begint

Uit een onderzoek van de toezichthouder bleek dat de AIVD een enkele keer DNA had verzameld om een identiteit van iemand vast te stellen. Omdat de vraag rees of dat is toegestaan onder de huidige wet, stelt de minister nu voor dat de AIVD een eigen, geheime en onbeperkte DNA-databank opzet waarin profielen van wie dan ook in principe eindeloos mogen worden opgeslagen.

De minister geeft ook hier een vrijbrief zonder dat er een enkel onderzoek gedaan is dat het nut of de noodzaak aantoon. Alleen een nachtelijk Kamerdebat met slechts drie partijen heeft tot dit voorstel geleid.

Het is voorstelbaar dat de AIVD in staat wordt gesteld om met DNA een identiteit vast te stellen, maar het is nergens aangetoond dat daarvoor een eigen databank met in principe onbegrensde bewaartermijnen daarvoor noodzakelijk is. Personen die in de DNA databank worden opgenomen worden hier niet van op de hoogte gebracht, waarmee de inbreuk extra groot is. Alvorens deze bevoegdheid in een wet wordt vormgegeven, moet er een gedegen onderzoek naar nut, noodzaak en rechtsbescherming voor burgers worden gedaan.

4. Hanteer geen ontsleutelplicht voor verdachten.

Het wetsvoorstel maakt het mogelijk dat verdachten gedwongen worden hun passwords af te geven zodat gegevens ontsleuteld kunnen worden. Als de verdachte hieraan niet meewerkt, kan hij tot twee jaar gevangenisstraf veroordeeld worden. De minister zegt aan te sluiten bij de ontsleutelplicht zoals die in artikel 126m, zesde lid, Wetboek van strafvordering is opgenomen. Maar daar gaat het uitdrukkelijk niet om de verdachte zelf en dat maakt een enorm verschil. In een rechtsstaat mag een verdachte nooit gedwongen worden aan zijn eigen veroordeling mee te werken. Dit is vastgelegd in het Europees Verdrag voor de Rechten van de Mens (EVRM). De AIVD zou dit volgens dit wetsvoorstel straks toch kunnen eisen, zelfs zonder dat er een rechter aan te pas komt.

5. Verbied het doorgeven van informatie voor de opsporing van strafbare feiten.

De AIVD krijgt met het voorstel van de minister verregaande toegang tot ieders privéleven. Het doel is om de staatsveiligheid te waarborgen. Het opsporen van strafbare feiten is geen onderdeel van deze taak. Het Europese Hof voor de Rechten van de Mens heeft dit in een vonnis uitdrukkelijk vastgesteld.

Toch is in het wetsvoorstel opgenomen dat de AIVD strafbare feiten aan het OM kan doorgeven. In deze algemene formulering is dat zeer ongewenst. Het kan nooit de bedoeling zijn dat de politie via de omweg van de AIVD alles en iedereen geautomatiseerd op afwijkend gedrag kan controleren. Het moet de AIVD expliciet verboden worden strafbare feiten aan het OM door te geven tenzij deze samenhangen met de staatsveiligheid.

6. Neem een horizonbepaling in het voorstel op.

Bevoegdheden die een forse inbreuk op de privacy van mensen betekenen, kunnen niet zomaar onbeperkt geldig zijn. Zeker niet als de AIVD nog *"ervaring moet opdoen"* (p.202 MvT) met wat ze eigenlijk met de bevoegdheden aan moet. In het wetsvoorstel zou daarom een horizonbepaling moeten worden opgenomen dat ingrijpende bevoegdheden automatisch na twee jaar vervallen. Als de minister die bevoegdheden wil verlengen, zal de minister met een voorstel hiervoor, onderbouwd met een evaluatie, opnieuw langs het parlement moeten.

De Eerste Kamer heeft dit in een motie ook geadviseerd. Een horizonbepaling is staande praktijk in andere landen, waaronder bijvoorbeeld de Verenigde Staten.

7. Verkort bewaartermijnen.

In het wetsvoorstel zijn bewaartermijnen opgenomen die veel te lang zijn. Daarmee alleen al is de wet in strijd met het Europees Verdrag voor de Rechten van de Mensen en het Internationaal Verdrag inzake Burgerrechten en Politieke rechten. Gegevens mogen slechts verzameld en bewaard worden als dat noodzakelijk is. In het nieuwe wetsvoorstel mogen gegevens zelfs tot 3 jaar bewaard worden, zelfs als al is vastgesteld dat ze niet relevant zijn. Het feit dat ze niet relevant zijn, betekent al dat de noodzaak om ze te bewaren vervalt.

Ook het bewaren van DNA profielen in de geheime DNA-databank kan met dit wetsvoorstel oneindig worden verlengd. De expliciete doelstelling voor het gebruik van DNA volgens dit wetsvoorstel is om de identiteit vast te stellen. Als de identiteit is vastgesteld, vervalt de noodzaak om het profiel te bewaren.

8. Maak het oordeel van de toezichthouder bindend

In het model van de minister wordt voorgesteld dat de minister een besluit nogmaals moet overwegen als de toezichthouder wijst op onrechtmatigheden. Dat is een zeer zwakke bescherming van fundamentele rechten. De minister kan immers na even nagedacht te hebben gewoon de onrechtmatige werkwijze voortzetten. Iets wat op dit moment dus ook al gebeurt. (Zie ook punt 10.) De toezichthouder zit er dan voor spek en bonen bij. Voor het waarborgen van fundamentele rechten van burgers, moeten de aanbevelingen en conclusies van de toezichthouder (CTIVD) bindend zijn.

De commissie Dessens *"acht het niet wenselijk dat de Wiv de mogelijkheid openlaat dat ministers een rechtmatigheidsoordeel van de CTIVD naast zich neer leggen. Als de CTIVD tot de conclusie komt dat een afgegeven last onrechtmatig is, moet de dienst de uitvoering van deze bijzondere bevoegdheid, voor zover deze op dat moment al is aangevangen, direct staken."* (blz. 101) De commissie concludeert dat oordelen van de toezichthouder bindend moeten zijn. Uiteraard kan dit bindend oordeel ook van de rechter komen zodra die een rol bij de inzet van bevoegdheden wordt toebedeeld.

9. Wees zo transparant mogelijk, zodat controle achteraf mogelijk wordt

De commissie Dessens schrijft hierover: *"Een zo groot mogelijke mate van transparantie draagt bij aan maatschappelijk vertrouwen en draagvlak voor het werk van de diensten. Tegelijkertijd draagt transparantie bij aan de waarborging van grondrechten."* (blz. 133) Transparantie is één van de belangrijkste waarborgen voor

onze vrijheden, omdat controle achteraf mogelijk wordt. Daarom zouden de volgende elementen in de herziene wet opgenomen moeten worden.

a. De minister publiceert jaarlijks statistieken over het aantal operaties waarbij bijzondere bevoegdheden zijn ingezet, het aantal toestemmingsverzoeken en hoeveel daarvan zijn afgewezen, het aantal taps uitgesplitst naar soort en communicatiemedium, en het aantal bevragingen van gegevens bij bedrijven en organisaties.
b. De AIVD stelt personen actief in kennis over alle bijzondere bevoegdheden die tegen hen zijn ingezet. De AIVD doet dit uiterlijk vijf jaar nadat de operatie is afgerond. De CTIVD controleert deze notificatieplicht.
c. Het verbod voor organisaties om jaarlijks geaggregeerde statistieken te publiceren over bevragingen door de AIVD verdwijnt.

10. Laat de rechter vooraf de inzet van bijzondere bevoegdheden goedkeuren

De commissie Dessens stelt dat het toezicht op en het toestemming geven voor de inzet van bijzondere bevoegdheden versterkt moet worden (blz. 56). Daarbij heeft het Europese Hof voor de Rechten van de Mens *"herhaaldelijk een voorkeur uitgesproken voor preventief rechterlijk toezicht op vormen van 'secret surveillance'"* (blz. 89). In het voorstel van minister Plasterk wordt als hoofdlijn voorgesteld dat de minister gefaseerd en beter geïnformeerd toestemming moet geven. Dat zal geen betere bescherming van grondrechten van burgers geven.

a. De AIVD blijkt zich maar matig aan de wet te houden. Uit rapportage van de toezichthouder CTIVD (toezichtsrapport nr. 40, 2014) blijkt dat in een steekproef zeker 17 keer onrechtmatig en 6 keer onzorgvuldig gehandeld is. De grootte van de steekproef is niet bekend gemaakt. De conclusie van de CTIVD dat *"in de meerderheid van de operaties de afluisterbevoegdheid op een rechtmatige en zorgvuldige wijze wordt uitgeoefend"* (blz. iv), is natuurlijk niet geruststellend. Als men zich 'over het algemeen' aan de wet houdt, zijn de rechten van burgers 'over het algemeen' dus niet gewaarborgd.

   De inlichtingen- en veiligheidsdiensten mogen nu al ongericht informatie verzamelen en doorzoeken, zolang die communicatie door de ether gaat. Juist hierbij blijken zowel de AIVD als de MIVD er een onrechtmatige werkwijze op na te houden (toezichtsrapport nr. 40, blz. 14 en verder). Er wordt te gemakkelijk in de metadata en inhoudelijke communicatie gegrasduind, terwijl dat op basis van de huidige wet aan strenge criteria moet voldoen. De toezichthouder meldt deze onrechtmatige werkwijze bij de minister, maar die onderneemt *"in overleg met de Tweede Kamer"* geen actie. (blz. 16) Zowel de minister als de Tweede Kamer tolereren deze onrechtmatige handelswijze en laten de burgers met hun grondrechten in de kou staan.

   Het fundamentele recht op privacy is dus niet gegarandeerd in het huidige model. Zeker niet waar het ongerichte verzameling van communicatie betreft. Het nieuwe model zal gezien bovenstaand voorbeeld ook geen betere garantie geven dat de AIVD en de MIVD zich dan wel aan de wet zullen houden. Alleen het inperken van bevoegdheden van de inlichtingendiensten en een oordeel van een onafhankelijk instantie als een rechter kan de grondrechten van burgers beschermen. Daar hebben we rechters ook voor.

b. Het briefgeheim wordt als enige communicatiemiddel door de Grondwet beschermd in artikel 13. Als de AIVD een postpakket of brief wil openen, moet het hiervoor toestemming vragen aan de rechter. Uit geen enkel toezichtsrapport blijkt dat zich hier knelpunten voordoen. De Grondwet dient in dit verband dan ook techniek-onafhankelijk te worden gemaakt. Artikel 13 dient aangepast te worden zodat alle vormen van communicatie tussen mensen door de Grondwet worden beschermd. Een rechterlijke toets is altijd noodzakelijk om daar inbreuk op te maken.
c. Het Europese Hof heeft onlangs geoordeeld in een zaak die de Telegraaf had aangespannen, dat de Wiv 2002 in strijd is met het Europees Verdrag voor de Rechten van de Mens (EVRM) omdat een externe toets ontbreekt. Volgens het Hof is een extern oordeel noodzakelijk, vóórdat bijzondere bevoegdheden worden ingezet. Dit vonnis dient breed geïnterpreteerd te worden en als zodanig in het wetsvoorstel terug te komen.
d. Oud-hoofd van de AIVD, Sybrand van Hulst, zegt in een uitzending van Radio Reporter (vanaf minuut 27) dat in de tien jaar dat hij baas van de AIVD (voorheen BVD) was, er nog nooit een minister toestemming voor de inzet van bijzondere bevoegdheden heeft geweigerd. Toch constateert de toezichthouder achteraf veel onrechtmatigheden. Ook hieruit blijkt dat het toestemmingsmodel waarbij de minister toestemming moet geven, de rechten van burgers niet beschermt tegen ongeoorloofde inbreuken door de AIVD.
e. In het wetsvoorstel wordt de toezichthouder geacht als onafhankelijke autoriteit te monitoren of de inzet van bevoegdheden rechtmatig is en daar vervolgens de minister op aan te spreken. De toezichthouder wordt zo medeverantwoordelijk gemaakt voor besluiten over de inzet. Dat vertroebelt het onafhankelijk toezicht achteraf, want de toezichthouder zal dan ook over haar eigen rol moeten oordelen. Door de inzet van een onafhankelijk rechter die vooraf een oordeel geeft, blijft de toezichthouder onafhankelijk en kan achteraf nog steeds de werkwijze en de genomen besluiten aan een kritisch oordeel onderwerpen.
f. De commissie Dessens constateert (p. 90) dat *"in de landen om ons heen de afgelopen decennia een ontwikkeling valt waar te nemen in de richting van meer extern toezicht vooraf op de inzet van inlichtingenmiddelen die een inbreuk maken op grondrechten. Deze ontwikkeling komt ook tot uitdrukking in een aanbeveling van de Parlementaire Assemblee van de Raad van Europa uit 1999 waarin een voorkeur wordt uitgesproken voor rechterlijk toezicht vooraf op elke inbreuk op grondrechten door I&V-diensten. Ook in de wetenschappelijke literatuur over toezicht op inlichtingen- en veiligheidsdiensten valt een zekere voorkeur te bespeuren voor preventief rechterlijk toezicht."*

11. Maak ook voor de uitwisseling van gegevens met andere landen een rechterlijke toets noodzakelijk

Vorig jaar bleek op pijnlijke wijze dat de MIVD met een sleepnet informatie verzamelt voor de Amerikaanse inlichtingendienst NSA. Zonder dat iemand het wist werden er 1,8 miljoen telefoongespreksgegevens aan de Amerikanen overhandigd. De toezichthouder beoordeelt deze werkwijze als onrechtmatig: *"De Commissie is van oordeel dat de huidige werkwijze van de MIVD niet in overeenstemming is met de Wiv 2002 en geen invulling geeft aan de waarborgen die in de wet besloten liggen. Deze werkwijze is derhalve onrechtmatig."* (toezichtsrapport nr. 38, blz. 35)

Gegevens mogen volgens de huidige wet na het verzamelen alleen gebruikt worden als aan criteria van noodzakelijkheid, proportionaliteit en subsidiariteit is voldaan. Bovendien moet er toestemming gegeven

worden door de minister. De gehele verzameling telefoongegevens zomaar aan de Amerikanen geven voldoet hier natuurlijk niet aan, ook omdat het merendeel communicatie van onverdachte burgers zal bevatten. Welke criteria de Amerikanen hanteren om de gegevens vervolgens te gebruiken, is onbekend. Mogelijk zijn de gegevens gebruikt om drone-aanvallen uit te voeren.

De wettelijke criteria zijn dus niet gevolgd en de privacy van burgers is met deze werkwijze duidelijk geschonden. Dus ook hier zijn met het toestemmingsmodel waarbij de minister toestemming geeft, de rechten van burgers niet gegarandeerd. (Zie ook punt 10.) Om roekeloos handelen van de inlichtingendiensten (en de minister) te voorkomen, dient een verzoek om gegevens met andere landen te delen altijd door een onafhankelijk rechter getoetst te worden.

12. Steek geld en energie in effectieve maatregelen

In het boek 'Theater van de angst' van terrorisme-expert Beatrice de Graaf wordt het inlichtingenwerk in vijf heldere stappen verdeeld. 1. inventariseren van behoeften; 2. verzamelen van inlichtingen; 3. verwerking van binnengekomen gegevens; 4. analyse, evaluatie, integratie en productie van het vergaarde materiaal zodat er een gereed intelligence-product ontstaat en 5. verspreiding van het product naar de afnemers.

Ook in dit wetsvoorstel wordt net als in het eerdere debat ingezoomd op stap twee, terwijl uit vrijwel alle aanslagen van de afgelopen jaren blijkt dat er duidelijk problemen liggen bij stap vier en vijf. Door het toestaan van ruimere bevoegdheden bij stap twee worden de problemen bij stap vier en vijf niet opgelost en de mogelijke problemen bij stap drie zelfs vergroot door de extra toevloed van gegevens.

Extra geld steken in nieuwe technologie om onverdachte burgers massaal af te luisteren, is geen zinvolle strategie voor meer veiligheid. Het geld, de mankracht en de energie kan veel effectiever worden besteed, zoals investeren in verbetering van analyse en evaluatie van gegevens die allang voorhanden zijn, maar waar tot nu toe onvoldoende op wordt geacteerd.

Vriendelijke groet,

Reinout Barth,
Privacy Barometer.

Reactie Vrijschrift op internetconsultatie concept-voorstel Wet inlichtingen en veiligheidsdiensten 2015

Inleiding

Over Vrijschrift

Vrijschrift werkt aan bewustwording van de economische en maatschappelijke betekenis van vrije kennis en cultuur voor onze samenleving. Vrijschrift heeft een beschermende en bevorderende rol voor informatievrijheid.

Adres:

Stichting Vrijschrift

Trekwei 7, 8711 GR Workum

Contactpersoon:

mr. drs. W.H. van Holst

Opbouw

Deze positiebepaling is verdeeld in algemene observaties over het concept-wetsvoorstel in zijn algemeenheid en de de volgende specifieke elementen van het wetsvoorstel:

- het verkennen van en heimelijk binnendringen in geautomatiseerde werken;
- het onderzoek van communicatie;
- informatie- en medewerkingsplicht aanbieders van communicatiediensten bij de verwerving van telecommunicatie en telecommunicatiegevens (gezamenlijk te behandelen met het onderzoek van communicatie);
- bijzondere bepalingen inzake geautomatiseerde data-analyse;
- en de samenwerking met inlichtingen- en veiligheidsdiensten van andere landen.

Wij behandelen deze bevoegheden in hun algemeenheid en per bevoegdheid in hun verhouding tot de uitingsvrijheid, de vrijheid om informatie te vergaren en overige grondrechten.

Algemene observaties

Kerntaken van de inlichtingen- en veiligheidsdiensten zijn de bescherming van de democratische rechtsstaat tegen aantastingen daarvan langs ondemocratische weg, bescherming van de internationale rechtsorde en bescherming van de territoriale integriteit van het Koninkrijk der Nederlanden. Hier vloeit logischerwijze uit voort dat, in het spanningsveld tussen het verzamelen van inlichtingen en de democratische rechtsstaat, de grondrechten en burgerlijke vrijheden niet verder aangetast mogen worden dan strikt noodzakelijk voor het beschermen van de democratische rechtsstaat. De bevoegdheden van inlichtingen- en veiligheidsdiensten zijn middelen die ondergeschikt zijn aan dit doel Uitbreiding of inzet van bevoegdheden die niet voldoen aan elementaire proportionaliteitsvereisten zijn een minstens zo grote bedreiging voor de democratische rechtsstaat als welke andere interne of externe bedreiging hiervan.

De activiteiten van de inlichtingen en veiligheidsdiensten kunnen, zeker zoals voorgesteld, de volgende grondrechten raken:

- de bescherming van de persoonlijke levenssfeer
- vrijheid van vereniging en vergadering
- godsdienstvrijheid
- uitingsvrijheid
- de vrijheid om informatie te vergaren
- het recht op een eerlijke procesgang en
- het recht op gelijke behandeling.

Wellicht ten overvloede: de wetenschap geobserveerd te (kunnen) worden leidt tot gedragsveranderingen. In een samenleving waarin geen aspect van het leven onberoerd wordt gelaten door informatietechnologie leidt een verruiming van surveillancebevoegdheden tot terughoudendheid in het vergaren van informatie, het bijwonen van bijeenkomsten en religieuze erediensten. Gezien de huidige focus van de inlichtingendiensten op islamistisch extremisme is het daarbij voorzienbaar dat ethnische en religieuze minderheden buitenproportioneel geraakt zullen worden in eerdergenoemde grondrechten en burgerlijke vrijheden. Dit is onverenigbaar met het grondwettelijk recht op gelijke behandeling.

In zijn algemeenheid valt op dat de Memorie van Toelichting bij het concept-wetsvoorstel bovengenoemd spanningsveld op zijn best aanstipt, en weinig informatie biedt over de afwegingen bij voorbaat terzake hiervan. Het concept-wetsvoorstel zou baat hebben bij expliciete vermelding van bovengenoemde tegenstelling.

In het licht van het bovenstaande betwijfelt Vrijschrift in zijn algemeenheid of de voorgestelde uitbreiding van bevoegdheden wel proportioneel kan zijn zonder een effectieve uitbreiding van het toezicht en waar mogelijk introductie van rechterlijke toetsing van het gebruik van deze (uitgebreide) bevoegdheden vooraf, in het bijzonder daar waar het gaat over onderzoek op verzoek van andere inlichtingen- of veiligheidsdiensten. Zeker nu gebleken is dat de inlichtingen- of veiligheidsdiensten van bondgenoten zoals de Verenigde Staten en het Verenigd Koninkrijk zich bedienen van werkwijzen die onverenigbaar zijn met de proportionaliteitsvereisten van het Europees Verdrag voor de Rechten van de Mens (EVRM) en die van het Handvest van de Grondrechten van de Europese Unie (het Europees Handvest) had dit wetsvoorstel ambitieuzer kunnen en moeten zijn. Daar waar de Wiv 2002 in art. 13 nog veronderstelt dat ieder verzoek van een inlichtingen- of veiligheidsdienst van een bondgenoot voldoet aan proportionaliteitsvereisten, zou dit concept-wetsvoorstel logischerwijze een toetsing analoog aan de toetsing aan art. 12 lid 1 sub a en e t/m g en lid 2 sub a en e t/m i van de Wiv 2002 (of de gelijksoortige bepalingen in art. 18 van dit concept-wetsvoorstel), waar onderzoeken van de eigen inlichtingen- en veiligheidsdiensten aan dienen te voldoen, bevatten.

Positief is de voorgestelde bronbescherming van journalisten door middel van rechterlijke toetsing vooraf. Dit zou een evenzeer geschikt model zijn om de vertrouwelijkheid van de communicatie tussen verdachten en hun advocaten (en daarmee het recht op een eerlijke procesgang), de vertrouwelijkheid van communicatie met religieuze ambtsdragers en het medisch beroepsgeheim te waarborgen. Het is verbazingwekkend dat het concept-voorstel geen voorstellen ter zake bevat.

Verkennen van en heimelijk binnendringen in een geautomatiseerde werken

Het voorstel bevat een verontrustende uitbreiding van de bevoegdheden van de Wiv 2002 op dit terrein. De bestaande bevoegdheden van de Wiv 2002 zijn in het licht van de voortgeschreden automatisering van vrijwel alle maatschappelijke sectoren en de hoge vlucht van smartphones die vrijwel zonder uitzondering gevoelige persoonsgegevens bevatten al veel ingrijpender geworden

dan zij waren. Tegen die achtergrond zou het in de lijn der verwachtingen liggen dat een concept-wetsvoorstel voor vervanging van de Wiv 2002 regels zou bevatten om het verbod tot verzameling van gevoelige persoonsgegevens anders dan hoogstnoodzakelijk geen dode letter te doen worden. Dit concept-wetsvoorstel zwijgt hierover en stelt daarentegen een bevoegdheid voor om computersystemen van de omgeving van doelwitten van de inlichtingen- en veiligheidsdiensten binnen te dringen. Uit de MvT blijkt dat deze doelwitten geen eigenstandige bedreiging hoeven te vormen om desondanks doelwit van deze hoogst ingrijpende bevoegdheid te worden.

Het concept-wetsvoorstel gaat hierbij voorbij aan de eventuele onbedoelde neveneffecten en en onvoldoende duidelijk waarom de voordelen van een zó ingrijpend optreden van inlichtingen- en veiligheidsdiensten opwegen tegen de nadelen, al was het maar omdat veel van de nadelen in het geheel niet genoemd worden. Evidente voorbeelden van dergelijke nadelen zijn het risico van het onbedoeld verstoren van (kritische) organisatieprocessen door een dergelijke operatie. Het binnendringen, zelfs verkennend, van een computersysteem is niet mogelijk zonder dit systeem te wijzigen. Zeker in het geval van het heimelijk aftappen van communicatie vereist dit diepgaande veranderingen in computersystemen, met het onvermijdelijk daarmee gepaard gaande risico van ernstige verstoring hiervan, met mogelijk ernstige gevolgen voor vitale belangen van derden.

Daarnaast zijn inlichtingen- en veiligheidsdiensten nu al belanghebbenden bij het in stand houden van beveiligingsproblemen in (consumenten)apparatuur en wellicht zelfs actieve afnemer op de reeds bestaande zwarte markt voor beveiligingslekken. Beveiligingslekken die op zichzelf al een groot gevaar voor de democratische rechtsorde en/of de openbare orde kunnen zijn. Een werkelijk gemoderniseerde Wiv 2015 zou afwegingskaders dienen te bevatten hoe hiermee om te gaan.

Ook gaat het concept-wetsvoorstel onvoldoende in op de mate waarin computers, in het bijzonder smartphones, een dusdanig integraal onderdeel uitmaken van het leven van burgers dat een dergelijke heimelijke observatie een veel grotere inbreuk op de persoonlijke levenssfeer is dan traditionele observatie. Een burger heeft zijn of haar smartphone immers vrijwel altijd bij zich en bevat zijn of haar e-mail geschiedenis, SMS-berichten, bezochte locaties, voicemailberichten en veelal ook alle ingangen in sociale media.

Het concept-wetsvoorstel zou baat hebben bij aanvullende waarborgen ter zake van de reeds bestaande bevoegdheden van de inlichtingen- en veiligheidsdiensten. Vrijschrift ziet ter zake van de uitbreiding van de bevoegdheden vooral voorstellen voor middelen die door het doel niet kunnen worden geheiligd.

Onderzoek van communicatie

De Wiv 2002 verleent in artikel 27 uitsluitend een bevoegdheid voor ongerichte onderschepping van telecommunicatieverkeer aan de inlichtingen- en veiligheidsdiensten voorzover het niet-draadgebonden telecommunicatie betreft waarvan een van de eindpunten zich buiten Nederland bevindt omdat dit volgens de toenmalige stand der techniek niet mogelijk was om gericht te doen vinden. Dertien jaar later zijn de mogelijkheden van de techniek om dit wél gericht te doen plaatsvinden toegenomen. Uit zowel art. 8 EVRM en de artt. 7 en 8 van het Europees Handvest vloeit dan ook voort dat het eerder voor de hand ligt om naar aanleiding van deze voortgeschreden technologische ontwikkelingen afscheid te nemen van deze bevoegdheid dan om deze uit te breiden. Desondanks wordt in het concept-wetsvoorstel onder het mom van 'techniekonafhankelijkheid' er voor gekozen om dit wel te doen. Juist daar waar technologie medebepalend is voor de proportionaliteitsvraag, is een dergelijke ontwikkeling onbegrijpelijk.

Nadrukkelijk dient opgemerkt te worden dat er deze eeuw er zich in Europa veiligheidsincidenten en aanslagen hebben voorgedaan waarvan de betrokkenen niet reeds in beeld waren van

inlichtingen- en veiligheidsdiensten en waarbij een ongerichte dataverzameling bijgedragen zou hebben aan het voorkomen hiervan. Knelpunt blijkt keer op keer analyse, niet de beschikbaarheid van informatie.

Vrijschrift is van mening dat de reeds bestaande bevoegdheden van de Wiv 2002 in het licht van de stand van de techniek eerder te ruim dan ontoereikend zijn en dat uitbreiding van deze reeds te ruime bevoegdheden een te grote aantasting van grondrechten met zich meebrengt om dit wetsvoorstel geen frontale aanval op de democratische rechtsstaat te laten zijn.

Daarnaast is het onbegrijpelijk dat de medewerking van dienstverleners op het gebied van telecommunicatie wordt gevergd zonder dat er minimale technische vereisten voor het waarborgen van de vertrouwelijkheid, authenticiteit en integriteit van dergelijke medewerkingsverzoeken worden geïntroduceerd, zoals bijvoorbeeld in sommige buurlanden zoals Duitsland het geval is. Zeker nu het concept-wetsvoorstel de kring van norm-adressanten verruimt tot iedere partij die enige vorm van telecommunicatie mogelijk maakt (en daarmee vrijwel ieder huishouden of bedrijf in Nederland) maakt dit concept-wetsvoorstel de samenleving kwetsbaar voor malafide partijen die zich voordoen als functionaris van een inlichtingen- of veiligheidsdienst.

Bijzondere bepalingen inzake geautomatiseerde data-analyse

Volledig nieuw is art. 47 van het concept-wetsvoorstel, waarbij de MvT bijna terloops vermeldt dat dit noodzakelijk is nu er nieuwe technieken voorhanden zijn, het vanzelfsprekend is dat nieuwe technieken ingezet kunnen worden én dat het onvermijdelijk is dat dit resulteert in ongerichte onderzoeken door de inlichtingen- en veiligheidsdiensten. Vrijschrift is van mening dat indien en voorzover het inherent aan een onderzoekstechniek is dat deze leidt tot ongericht onderzoek, het vanzelfsprekend is dat de inlichtingen- en veiligheidsdiensten zich onthouden van een dergelijke onderzoekstechniek omdat deze inherent onverenigbaar is met de democratische rechtsstaat.

Daarnaast gaat het concept-wetsvoorstel volledig voorbij aan het feit dat met het verdrag van Lissabon het Europees Handvest van toepassing is geworden op de activiteiten van de Nederlandse inlichtingen- en veiligheidsdiensten. Met name art. 8 van het Europees Handvest legt eisen op aan de waarborgen verbonden aan data-analyse die in het concept-wetsvoorstel niet of onvoldoende geadresseerd worden. Waarover later meer.

Ter zake van door derden ter beschikking gestelde geautomatiseerde gegevensbestanden moet opgemerkt worden dat hiermee in combinatie met de (te vergaande, zie daarover later meer) bevoegdheden tot samenwerking met inlichtingen- en veiligheidsdiensten van andere landen een mogelijkheid ontstaat tot het 'witwassen' van massasurveillance via deze samenwerkingsverbanden.

Samenwerking met inlichtingen- en veiligheidsdiensten van andere landen

Zoals al in de algemene observaties opgemerkt zijn in het licht van de onthullingen van Edward Snowden over ongekende surveillance door de inlichtingen- en veiligheidsdiensten van de Verenigde Staten en het Verenigd Koninkrijk aanvullende waarborgen vereist ter zake van de samenwerking met de inlichtingen- en veiligheidsdiensten van andere landen. Bijzonder navrant daarbij is dat diverse NAVO-bondgenoten blijkbaar ongericht telecommunicatie van niet-ingezetenen aftappen en dit met elkaar delen, zodat zij gezamenlijk massasurveillance van eigen burgers realiseren, maar op het niveau van NAVO-lidstaat kunnen beweren dit niet te doen. Ook de geconstateerde praktijken uit het recente verleden van marteling door inlichtingen- en veiligheidsdiensten van een belangrijke NAVO-bondgenoot als de Verenigde Staten zijn in dit opzicht een onderwerp wat redelijkerwijze door het concept-wetsvoorstel geaddresseerd zou worden.
De MvT van het concept-wetsvoorstel onderkent dit slechts ten dele en in het voorsgestelde art. 76 wordt de vraag van het heroverwegen van een samenwerking overgelaten aan het hoofd van

desbetreffende inlichtingen- of veiligheidsdienst. Wij zijn van mening dat de hoofden van de diensten te zeer gevangen kunnen zijn in het quid quo pro van de internationale samenwerking dat zij redelijkerwijze niet in staat geacht kunnen worden om een dergelijke heroverweging op objectieve wijze gestalte te doen geven. Vrijschrift bepleit de mogelijkheid van een gerechtelijke procedure ter zake waarbij een specifieke rechtbank de minister kan gelasten, zonder dat deze verplicht kan worden het bestaan van een samenwerking te onthullen, om deze voor een beperkte termijn op te schorten of terug te brengen als er voldoende aanleiding is om te twijfelen aan de eerbiediging van de mensenrechten door het desbetreffende land.
Zoals al eerder opgemerkt in de algemene observaties, is het niet meer realistisch om geen proportionaliteitstoetsing op verzoeken van inlichtingen- en veiligheidsdiensten van andere landen plaats te doen vinden. Art. 77 van het concept-wetsvoorstel zou hiervoor een logische plaats zijn.
Tot slot moet opgemerkt worden dat bij het verstrekken van inlichtingen die ook persoonsgegevens bevatten aan inlichtingen- en veiligheidsdiensten van andere landen buiten de Europese Unie uit art. 8 van het Europees Handvest voortvloeit dat deze onder onafhankelijk toezicht moeten staan dat vergelijkbaar is met het onafhankelijk toezicht op de eigen inlichtingen- en veiligheidsdiensten. Het concept-wetsvoorstel rept hier niet over.

Boekx
Media & Intellectual Property

Boekx Advocaten

Leidsegracht 9
Postbus 15988
1001 NL Amsterdam

T +31 20 528 95 32
F +31 20 528 95 37

www.boekx.com

De Minister-President, Minister van Algemene Zaken
De Minister van Binnenlandse Zaken en Koninkrijksrelaties
De Minister van Defensie
De Minister van Veiligheid en Justitie

Amsterdam, 31 augustus 2015

Inzake: Reactie op concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX
Aanbevelingen Studiecommissie Journalistieke Bronbescherming

Excellenties,

De Studiecommissie Journalistieke Bronbescherming[1] van de Vereniging voor Media- en Communicatierecht heeft kennis genomen van het concept-wetsvoorstel voor een Wet op de inlichtingen- en veiligheidsdiensten 20xx (hierna: Wiv20xx), dat ter consultatie is voorgelegd.

De Studiecommissie ziet fundamentele juridische problemen en doet in totaal 19 aanbevelingen voor aanpassingen.

---

[1] De Studiecommissie bestaat uit de volgende leden:
- mr. T. Bruning, secretaris Nederlandse Vereniging van Journalisten;
- prof. dr. N. Helberger, hoogleraar Informatierecht, IvIR, Universiteit van Amsterdam;
- prof. dr. A.W. Hins, hoogleraar Mediarecht, Universiteit Leiden;
- mr. G. Kemper, advocaat;
- mr. W.F. Korthals Altes, senior-rechter Rechtbank Amsterdam, Visiting Professor New York Law School;
- mr. B. Le Poole, advocaat, Le Poole Bekema;
- mr. P. Malherbe, journalist en docent journalistiek, Universiteit van Amsterdam en Hogeschool voor de Kunsten Utrecht;
- dr. T. McGonagle, senior onderzoeker IvIR, Universiteit van Amsterdam;
- mr. S.P. Poppelaars, promovenda Staatsrecht, Radboud Universiteit Nijmegen;
- dr. Ch. Samkalden, advocaat, Prakken d'Oliveira;
- mr. O. Trojan, advocaat, Bird & Bird;
- mr. J.P. Vogel, director juridische zaken Sanoma Media Netherlands B.V.;
- mr. O.M.B.J. Volgenant, advocaat, Boekx Advocaten; en
- prof. dr. D. Voorhoof, hoogleraar Mediarecht, Universiteit Gent en Universiteit Kopenhagen.

In het najaar van 2014 heeft de Nederlandse regering twee wetsvoorstellen[2] ingediend om gehoor te geven aan de opdracht die het EHRM al geruime tijd geleden aan Nederland heeft gegeven: het waarborgen van journalistieke bronbescherming, met name in de vorm van rechterlijke toetsing voorafgaand aan het inzetten van opsporings- of dwangmiddelen tegen journalisten. In de toelichtingen op deze wetsvoorstellen werd de intentie geuit de rechtsbescherming in Nederland in lijn te brengen met die Europese jurisprudentie. De teksten van die twee wetsvoorstellen voldeden daar echter op belangrijke punten niet aan.

Bij brief van 22 oktober 2014 heeft de Studiecommissie reeds tien aandachtspunten geïdentificeerd. Voor de overzichtelijkheid worden die aandachtspunten hieronder herhaald.

Aanbevelingen 22 oktober 2014

1. De wettelijke bescherming dient te gelden tegenover alle overheidsdiensten die zich met onderzoek en opsporing bezighouden. De twee wetsvoorstellen richten zich echter uitsluitend op strafzaken (OM en politie) en de AIVD en de MIVD. Er wordt onvoldoende gewaarborgd dat ook andere overheidsdiensten, bijvoorbeeld de FIOD, zich hier aan houden. *Betreft beide wetsvoorstellen.*

2. De voorgenomen wijziging van het Wetboek van Strafvordering bestrijkt een aantal specifieke strafvorderlijke dwangmiddelen. Doordat het voorstel geen algemeen geformuleerd recht op bronbescherming in de wet vastlegt, maar het per dwangmiddel regelt, rijst de vraag of dit nu wel voor álle dwangmiddelen geldt. De wettekst dient dit te verduidelijken en in alle omstandigheden van strafvorderlijke dwangmiddelen het recht op journalistieke bronbescherming te waarborgen. *Betreft Sv.*

   Voorbeeld: De voorgestelde 'hackwet' (wetsvoorstel Computercriminaliteit III) lijkt niet te onderkennen dat journalisten een bijzondere positie hebben. Hoe wordt gewaarborgd dat uitsluitend in een computer van een journalist wordt binnengedrongen nadat een rechter heeft vastgesteld dat dat noodzakelijk is om te voorkomen dat aan een zwaarder belang een onevenredig grote schade wordt toegebracht?

3. Het wetsvoorstel tot wijziging van het Wetboek van Strafvordering introduceert het begrip 'publicist in het kader van nieuwsgaring'. Dat is onwenselijk. De Raad van State constateert in zijn advies van 30 augustus 2013 terecht dat het ongewenst is dat er verschil in reikwijdte is ten aanzien van de groep beschermingsgerechtigden in beide wetsvoorstellen. Het nieuwe begrip 'publicist in het kader van nieuwsgaring' heeft geen basis in de toepasselijke regelgeving of jurisprudentie en zal mogelijk tot misverstanden bij de politie en het OM en tot ongewenste geschillen bij de rechter aanleiding geven. Ook vergelijkbare buitenlandse wetten kennen dit begrip niet. Onduidelijk is daarom wie precies als 'publicist in het kader van nieuwsgaring' zal worden aangemerkt. De zinsnede 'publicist in het kader van nieuwsgaring'

[2] Wetsvoorstel TK 34 027: Wijziging van de Wet op de Inlichtingen- en veiligheidsdiensten 2002 in verband met de invoering van een onafhankelijke bindende toets voorafgaand aan de inzet van bijzondere bevoegdheden jegens journalisten, welke gericht is op het achterhalen van hun bronnen, en Wetsvoorstel TK 34 032: Wijziging van het Wetboek van Strafvordering tot vastlegging van het recht op bronbescherming bij vrije nieuwsgaring (bronbescherming in strafzaken).

dient te vervallen en het begrip 'journalist' dient in alle regelgeving dezelfde inhoud te hebben. De Memorie van Toelichting dient een brede en open definitie van het begrip 'journalist' te geven, waarbij aangesloten kan worden bij de invulling van dat begrip in *Recommendation R(2000)7* die in beide toelichtingen wordt aangehaald. *Betreft beide wetsvoorstellen.*

4. Het begrip 'bron' is ten onrechte beperkt tot 'personen die gegevens ter openbaarmaking aan een journalist hebben verstrekt *onder de voorwaarde* dat de verstrekking niet tot hen kan worden herleid'. In de journalistieke praktijk zijn er vele gevallen waarin de bron beschermd dient te blijven zonder dat er daartoe een expliciete afspraak is gemaakt. De voorgestelde beperking is onwenselijk en bovendien expliciet in strijd met *Recommendation R(2000)7*. De beperking dient uit de wetsvoorstellen te worden geschrapt. *Betreft beide wetsvoorstellen.*

5. Er is onvoldoende gewaarborgd dat hoger beroep kan worden ingesteld en dat de overheidsdienst zich ondertussen geen toegang tot de gezochte informatie kan verschaffen. Als de bron eenmaal bekend is geraakt bij de overheidsdienst, kan die informatie immers niet meer 'ongedaan' worden gemaakt. De wet dient derhalve zowel waarborgen te bieden voor een effectief hoger beroep als voor journalistieke bronbescherming totdat een rechterlijk vonnis kracht van gewijsde heeft. *Betreft Sv.*

6. De mogelijkheid van verzegeling van informatie gedurende de procedure van rechterlijke toetsing wordt in de toelichting genoemd, maar niet in de wet vastgelegd. Ook dit is een lacune in de wet. *Betreft Sv.*

7. Waarom wordt niet wettelijk vastgelegd dat de rechter modaliteiten kan aanbrengen in de opsporingsmethoden, of beperkingen kan aanbrengen in het af te geven materiaal?[3] Ook op dit punt dient te wet waarborgen te bieden. *Betreft beide wetsvoorstellen.*

8. De toelichting op het wetsvoorstel tot wijziging van de Wiv 2002 wijst erop dat de inlichtingendiensten zelf de beoordeling moeten maken of ze te maken hebben met een journalist. Dat lijkt inherent risicovol. Het verdient aanbeveling in de regelgeving op te nemen dat de inlichtingendiensten in dit verband een stevige onderzoeksplicht hebben: zij zullen gedegen moeten onderzoeken of iemand werkzaam is als journalist, en dit adequaat moeten vastleggen. In geval er redelijkerwijs ruimte is om te twijfelen of iemand journalist is, zal altijd een verzoek aan de Rechtbank Den Haag moeten worden gedaan. Het wetsvoorstel dient op dit punt aangevuld te worden. *Betreft Wiv 2002.*

9. Het wetsvoorstel tot wijziging van de Wiv 2002 verplicht inlichtingendiensten rechterlijke toestemming te vragen wanneer hun werk is *'gericht op het achterhalen van de bron'*. Dit impliceert – zonder dat de toelichting dit goed duidelijk maakt – dat de inlichtingendiensten

[3] zoals expliciet voorgeschreven in alinea 92 van het *Sanoma*-arrest, EHRM 14 september 2010.

wel onderzoek naar journalisten zouden mogen doen wanneer dat onderzoek niet is 'gericht op het achterhalen van de bron'. Dat zou echter een zeer onwenselijke lacune in de rechtsbescherming van bronnen en journalisten opleveren. Immers, als eenmaal kennis over een bron aanwezig is bij een overheidsdienst, kan die kennis niet meer ongedaan worden gemaakt. Het op grote schaal ongericht verzamelen van data (de schepnetmethode) verhoudt zich niet met journalistieke bronbescherming. Wanneer overheidsdiensten allerlei communicatiegegevens van journalisten verzamelen, zal daar veel informatie bij zitten die tot bronnen te herleiden is. Het recht op bronbescherming zou een wassen neus zijn als deze bescherming beperkt zou worden tot het vragen van rechterlijke toetsing in een fase dat een overheidsdienst de informatie al lang in huis heeft. *Betreft Wiv 2002.*

10. Voor (professionele) journalisten gelden allerlei wettelijke regels, ethische (beroeps)regels, plichten en verantwoordelijkheden. Van geval tot geval zal beoordeeld moeten worden hoe bijvoorbeeld invulling moet worden gegeven aan het verlenen van wederhoor voordat een journalist tot publicatie overgaat. Het overtreden van geldende normen kan civielrechtelijke en zelfs strafrechtelijke consequenties hebben. Dat is voldoende. Het recht op bronbescherming dient niet beperkt te worden tot journalisten die zich aan alle wettelijke en ethische normen hebben gehouden, voor zover dat al kan worden vastgesteld. Dat zou een onwerkbare toets opleveren, die niet in lijn is met de jurisprudentie van het EHRM. *Betreft beide wetsvoorstellen.*

Deze tien bezwaren zijn in een Rondetafelgesprek op 5 december 2014 nader toegelicht aan de Vaste Commissie voor Veiligheid en Justitie, die hierover op 12 december 2014 vragen heeft gesteld.[4] Bovenstaande tien punten zijn allemaal vrijwel letterlijk benoemd door de Kamerleden. Sindsdien ligt de behandeling van deze twee wetsvoorstellen stil. Deze vragen vanuit de Tweede Kamer zijn dus nog niet beantwoord. Bovenstaande tien aandachtspunten zijn vervolgens helaas ook niet geadresseerd in het nu ter consultatie voorgelegde wetsvoorstel Wiv20xx.

Artikel 24.4 van het wetsvoorstel Wiv20xx bevat de tekst van het wetsvoorstel uit 2014. Voor de toelichting bij dit artikel 24.4 wordt kortweg verwezen naar de Memorie van Toelichting bij het wetsvoorstel uit 2014.[5]

Tussenconclusie is dat bovenstaande tien aandachtspunten, die worden gedeeld door de Vaste Commissie voor Veiligheid en Justitie van de Tweede Kamer, nog steeds geadresseerd moeten worden om het recht op journalistieke bronbescherming te borgen op een wijze die toetsing door het EHRM kan doorstaan. Het huidige wetsvoorstel Wiv20xx voldoet niet aan de eisen die het EVRM en de rechtspraak van het EHRM stellen.

[4] Verslag, vastgesteld 12 december 2014, Tweede Kamer 2014/2015, 34 032, nr. 6.

[5] Op pagina 35 van de Memorie van Toelichting op de Wiv20xx staat te lezen: *Kortheidshalve wordt voor een nadere uiteenzetting verwezen naar de desbetreffende kamerstukken.*

Het afluisteren en volgen van journalisten en het binnendringen van computersystemen van redacties en journalisten zijn zeer vergaande bevoegdheden, met een groot risico dat de diensten veel meer informatie vinden die tot bronnen te herleiden is dan wenselijk is. Dat de inlichtingendiensten middelen inzetten om bronnen van journalisten te achterhalen is niet denkbeeldig. Toen De Telegraaf in 2006 publiceerde over 'AIVD-geheimen bij de drugsmaffia' ging de AIVD direct de betrokken journalisten afluisteren, volgen en hun telecomgegevens opvragen. Deze kwestie leidde tot een veroordeling van Nederland door het EHRM in 2012. En toen De Telegraaf in 2009 publiceerde hoe de 'AIVD faalde rond Irak' ging de AIVD wederom direct de journalisten afluisteren om hun bron te achterhalen. De CTIVD oordeelde achteraf dat dit niet proportioneel was, maar toen had de AIVD al voldoende informatie vergaard. [6] Deze kwestie is inmiddels aan het EHRM voorgelegd. De praktijk heeft de afgelopen jaren geleerd dat de AIVD een aantal malen aantoonbaar te ver is gegaan met het inzetten van bevoegdheden jegens journalisten.

De Studiecommissie is kritisch op het voorstel tot verruiming van de bevoegdheden van de inlichtingen- en veiligheidsdiensten, terwijl er niet tegemoet is gekomen aan de in 2014 reeds gesignaleerde tien aandachtspunten. Het inzetten van brede bevoegdheden om communicatie te onderscheppen heeft een *chilling effect* op de persvrijheid en de vrijheid van meningsuiting. Dit is recent door de Verenigde Naties erkend.[7]

De Studiecommissie Bronbescherming heeft het wetsvoorstel Wiv 20xx gelezen en ziet de volgende negen aanvullende aandachtspunten.

1. Nut en noodzaak van de voorgestelde forse uitbreiding van bevoegdheden van de inlichtingen- en veiligheidsdiensten zijn niet onderbouwd. In de Memorie van Toelichting valt te lezen dat ongeveer 90% van alle telecommunicatie via kabelnetwerken verloopt. De diensten hebben momenteel niet de bevoegdheid tot ongerichte interceptie van de kabel. De regering heeft niet onderbouwd waarom de huidige bevoegdheden, waaronder de huidige bevoegdheid tot gerichte interceptie (artikel 25 Wiv2002), niet voldoen. Zonder onderbouwing valt niet in te zien waarom ongerichte bulk-interceptie (het sleepnet zoals voorgesteld in artikel 33 Wiv20xx) noodzakelijk zou zijn.[8] Artikel 33 Wiv20xx kan geschrapt worden.

2. Ongerichte bulk-interceptie stuit op fundamentele juridische bezwaren. Massa-surveillance botst met het grondrecht op privacy van alle burgers. Dat is in strijd met artikel 8 EVRM en artikelen 7 en 8 van het EU-Handvest van de Grondrechten. Bovendien kan het feit dat de gegevens worden bewaard en later worden gebruikt zonder dat de burger hierover wordt ingelicht het gevoel

[6] Hoge Raad 31 maart 2015, ECLI:NL:HR:2015:768.

[7] *Report of the Special Rapporteur to the Human Rights Council on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression*, 17 april 2013, A/HRC/23/40

[8] Dit wordt onderschreven door de CTIVD in haar jaarverslag 2014, p. 28: *Uitgangspunt zou moeten zijn dat eerst de noodzaak voor nieuwe bevoegdheden, ingegeven door tekortschietende effecten van de huidige bevoegdheden, overtuigend moet worden aangetoond voordat sprake kan zijn van een wettelijke uitbreiding. Deze effectiviteitstoets wordt ook ingegeven door de rechtmatigheidstoets die artikel 8 van het Europees Verdrag voor de Rechten van de Mens voorschrijft vanuit het oogpunt van privacybescherming.*

opwekken dat het privéleven constant in de gaten wordt gehouden. Het Hof van Justitie van de EU liet dit zwaar meewegen bij de beoordeling van de dataretentierichtlijn in 2014, en verklaarde die richtlijn mede hierom ongeldig.[9] De Nederlandse implementatie van die richtlijn werd op 11 maart 2015 door de rechter buiten werking gesteld, mede op vordering van de NVJ en mede op grond van de bezwaren die grootschalige opslag van communicatiegegevens oplevert voor journalistieke bronbescherming.[10]

3. De verplichting om mee te werken aan ontsleuteling van gegevens en aan het onderzoek van geautomatiseerde systemen kan een groot *chilling effect* hebben wanneer de diensten zich richten op systemen die juist functioneren dankzij het vertrouwen van de gebruiker in de veiligheid en versleuteling. Denk aan het Nederlandse klokkenluidersplatform Publeaks. Beveiligde journalistieke omgevingen zouden niet gedwongen moeten kunnen worden om mee te werken aan ontsleuteling.[11]

4. Voor journalisten is in artikel 24 lid 4 Wiv20xx voorzien in rechterlijke toetsing vooraf. Hoewel niet rechtstreeks van belang voor journalistieke bronbescherming, rijst de vraag waarom een dergelijke waarborg niet voor alle geheimhouders (inclusief advocaten, notarissen en artsen) in de wet opgenomen zou moeten worden. En ook voor het inzetten van bevoegdheden tegen niet-geheimhouders zal voorafgaande onafhankelijke toetsing een belangrijke waarborg opleveren. De Studiecommissie verwijst met instemming naar de tien aanbevelingen voor toezicht op de diensten zoals opgenomen in het recente IViR-rapport hierover.[12]

5. Het wetsvoorstel Wiv20xx maakt onvoldoende duidelijk hoe het vragen van voorafgaande toestemming van de Rechtbank Den Haag ex artikel 24 lid 4 Wiv20xx zich in de praktijk zal verhouden tot de zeer ruime geformuleerde bevoegdheden van de diensten, zoals bijvoorbeeld ongerichte bulk-interceptie (het sleepnet). Wanneer de diensten ongericht allerlei communicatiegegevens verzamelen, zal daar veel informatie bij kunnen zitten die tot bronnen te herleiden is (de bijvangst). Het recht op bronbescherming zou een wassen neus zijn als deze bronbescherming beperkt zou worden tot het vragen van rechterlijke toetsing in een fase dat een overheidsdienst de informatie al lang in huis heeft.[13] Dit is in strijd met de rechtspraak van het EHRM.[14] In ieder geval dient er te worden voorzien in een regeling voor het separeren van de bijvangst tot het moment dat de rechter zich heeft uitgesproken.

---

[9] Hof van Justitie van de Europese Unie 8 april 2014, gevoegde zaken *Digital Rights Ireland* en *Seitlinger* (zaken C-293/12 en C294/12).

[10] Vzr. Rechtbank Den Haag 11 maart 2015, ECLI:NL:RBDHA:2015:2498, *Privacy First c.s. / De Staat.*

[11] Dit betreft o.a. artikel 30, vijfde en achtste lid en artikel 41 Wiv20xx.

[12] *Ten standards for oversight and transparancy of national intelligence services*, IViR (Institute for Information Law), July 2015.

[13] Vzr. Rechtbank Den Haag 1 juli 2015, ECLI:NL:RBDHA:2015:7436, *Advocaten / De Staat*, r.o. 4.9: *Volgens de Staat kan als een journalistieke bron eenmaal bekend is, dit niet meer ongedaan gemaakt worden.*

[14] EHRM 22 november 2012, no. 39315/06, *De Telegraaf / Nederland,* eist *prior review by an independent body with the power to prevent or terminate it. Review post factum (...) cannot restore the confidentiality of journalistic sources once it is destroyed.*

6. De wijze waarop voorafgaande rechterlijke toetsing ex artikel 24 lid 4 Wiv20xx door de Rechtbank Den Haag zal worden verricht is niet uitgewerkt in het wetsvoorstel. Het verdient aanbeveling om dit te beleggen bij de Raadkamer van de sector Civiel van de Rechtbank Den Haag, zodat drie rechters gezamenlijk beslissen over het opzij zetten van de journalistieke bronbescherming. In zeer spoedeisende kwesties zou het oordeel van een Voorzieningenrechter kunnen worden gevraagd. De Studiecommissie raadt af de toetsing te beleggen bij een rechter-commissaris, ten eerste omdat deze dan alleen moet oordelen over vaak zeer complexe en gevoelige zaken, en ten tweede omdat de Raadkamer meer afstand heeft tot opsporing en vervolging dan de rechter-commissaris.

7. Het briefgeheim kan slechts worden doorbroken na toestemming van de rechter (artikel 29 Wiv20xx). Als deze procedure voor brieven kan worden gevolgd, dan zou een zelfde waarborg eenvoudig ook voor alle andere soorten communicatie in de wet opgenomen kunnen worden.

8. Het delen van gegevens met andere partijen, waaronder buitenlandse inlichtingendiensten (artikel 4 Wiv20xx) is met onvoldoende waarborgen omgeven. Uit 'ongeëvalueerde gegevens' als bedoeld in artikel 49 lid 3 Wiv20xx zullen bronnen van journalisten kunnen worden gedestilleerd. De wet dient voldoende waarborgen te bevatten om te voorkomen dat derden onderzoek kunnen doen waar de diensten zelf niet toe gerechtigd zijn.

9. De Memorie van Toelichting bij de Wiv20xx bevat geen specifieke toelichting op de journalistieke bronbescherming van artikel 24 lid 4, maar slechts een verwijzing naar de Memorie van Toelichting van een eerder wetsvoorstel. Dat is onwenselijk, want dit zal de uitleg van de wettelijke regeling van journalistieke bronbescherming onnodig complex maken. Het verdient aanbeveling om in de Memorie van Toelichting bij de Wiv20xx integraal de toelichting op de journalistieke bronbescherming op te nemen.

Nederland is de afgelopen jaren al drie keer veroordeeld wegens schending van het grondrecht van artikel 10 EVRM, in 2007 (*Voskuil*), 2010 (*Sanoma*) en 2012 (*De Telegraaf*). Bij brief van 7 december 2012[15] heeft de Minister van Binnenlandse Zaken de Tweede Kamer toegezegd de Wiv 2002 te wijzigen om journalistieke bronbescherming een wettelijke basis te geven, en te bezien hoe in de periode voordat de wet is aangepast in de praktijk zal worden voorzien in voorafgaand onafhankelijk toezicht. De Studiecommissie constateert dat het daadwerkelijk aanpassen van de wetgeving te lang op zich laat wachten (op de kop af vijf jaar sinds het *Sanoma*-arrest van het EHRM[16]), en dat de Staat

[15] Tweede Kamer 2012/2013, 30 977, nr. 49.

[16] EHRM (Grand Chamber) 14 september 2010, no. 38224/03 (*Sanoma/Nederland*): *Given the preventive nature of such review the judge or other independent and impartial body must thus be in a position to carry out this weighing of the potential risks and respective interests prior to any disclosure and with reference to the material that it is sought to have disclosed so that the arguments of the authorities seeking the disclosure can be properly assessed. The decision to be taken should be governed by clear criteria, including whether a less intrusive measure can suffice to serve the overriding public interests established. It should be open to the judge or other authority to refuse to make a disclosure order or to make a limited or qualified order so as to protect*

geen daadwerkelijke poging heeft ondernomen om te voorzien in voorafgaand onafhankelijk toezicht voor de periode tot de wet is aangepast. Uit het optreden van de Staat spreekt geen urgentie om consequenties te verbinden aan de drie veroordelingen door het EHRM. Dat is een onwenselijk signaal. De Staat zou veroordelingen door het EHRM serieuzer moeten nemen.

Te verwachten valt dat de parlementaire behandeling van het wetsvoorstel Wiv20xx nog geruime tijd in beslag zal nemen. De Studiecommissie roept de Staat op journalistieke bronbescherming op korte termijn te waarborgen en dit onderwerp niet te laten wachten op het wetsvoorstel Wiv20xx.

Het is van belang dat de Nederlandse wet de bescherming biedt die voorgeschreven wordt door artikel 10 lid 2 EVRM en de jurisprudentie van het EHRM. Onze aanbevelingen (inmiddels negentien in totaal) zijn er stuk voor stuk op gericht om de Nederlandse wettelijke regeling op dat niveau te brengen.

De Studiecommissie verzoekt U deze aanbevelingen mee te nemen bij de verdere parlementaire behandeling van de wetsvoorstellen.

Hoogachtend,
namens de Studiecommissie Journalistieke Bronbescherming,

O.M.B.J. Volgenant

---

sources from being revealed, whether or not they are specifically named in the withheld material, on the grounds that the communication of such material creates a serious risk of compromising the identity of journalist's sources. In situations of urgency, a procedure should exist to identify and isolate, prior to the exploitation of the material by the authorities, information that could lead to the identification of sources from information that carries no such risk.

T · ·Mobile·

LIFE IS FOR SHARING.

Ministerie van Binnenlandse Zaken en Koninkrijkrelaties en Ministerie van Defensie

Betreft: Internetconsultatie Wet op de inlichtingen- en informatiediensten 20xx

Den Haag, 31 augustus 2015

Geachte minister Plasterk,

Op 2 juli jl. is het Voorstel van Wet op de inlichtingen- en veiligheidsdiensten 20xx ter consultatie aangeboden. T-Mobile Netherlands B.V. (hierna T-Mobile) maakt graag gebruik van de mogelijkheid om haar zienswijze bij u neer te leggen.

T-Mobile begrijpt dat in het kader van de nationale veiligheid de bevoegdheden van de inlichtingen- en veiligheidsdiensten tegen het licht gehouden moeten worden, zeker gezien de technologische vooruitgang die Nederland niet ongemoeid heeft gelaten sinds 2002, het jaar waarin de Wet op de inlichtingen – en veiligheidsdiensten 2002 in werking is getreden.
T-Mobile is echter van mening dat de basis ten aanzien van de onderbouwing, afbakening en motivatie voor dit wetsvoorstel nog onvoldoende is.

Het wetsvoorstel en de bijbehorende Memorie van Toelichting roepen vele vragen op. Bij een aantal belangrijke onderdelen zijn er grote juridische en operationele vraagtekens te zetten voor wat betreft de haalbaarheid van het voorstel. In onderstaande zienswijze wordt zoveel mogelijk ingegaan op deze laatste elementen. T-Mobile denkt hierin echter niet uitputtend sluitend te kunnen zijn, gezien de eerder genoemde onduidelijkheden en hiaten in het voorstel.

Proportionaliteit
In het voorliggende wetsvoorstel worden de inlichtingen- en veiligheidsdiensten meer bevoegdheden gegeven. T-Mobile vraagt zich af of een dergelijke grote uitbreiding noodzakelijk en proportioneel is. De huidige regelgeving inzake het zetten van voice en data taps lijken prima te voldoen. Nadere onderbouwing voor de uitbreiding van bevoegdheden lijkt ons van essentieel belang omdat proportionaliteit ook rechtszekerheid betekent. Voor zowel de burger als de aanbieders van openbare communicatienetwerken. Overigens is er in Nederland nooit eerder een brede maatschappelijke discussie gevoerd over de noodzaak tot uitbreiding de huidige bevoegdheden. Een dergelijke discussie lijkt nu op gang te zijn gekomen door deze consultatieronde. Een discussie die door ons met belangstelling actief gevolgd gaat worden.

T-MOBILE NETHERLANDS BV
Adres: Waldorpstraat 60, 2521 CC Den Haag
Postadres: Postbus 16272, 2500 BG Den Haag
Telefoon: +31 (0)6 1409 5000 | Fax: +31 (0)6 1409 5024 | Internet: www.t-mobile.nl
Bank: Commerzbank Amsterdam 73.39.59.717 | KvK: Den Haag, 33265679

T · ·Mobile·

LIFE IS FOR SHARING.

Privacy

T-Mobile heeft de privacy van haar abonnees en het beschermen van data altijd tot een van haar hoogste prioriteiten gesteld. In de wet en de bijbehorende Memorie van Toelichting wordt de, door ons noodzakelijk bevonden, toetsing van het College Bescherming Persoonsgegevens gemist.

Op pagina 205 zou een hoofdstuk worden gewijd aan een privacy impact assessment. Er staat echter niet meer weergegeven dan 'PM'. Als de privacy assessment voltooid is, zou T-Mobile daar graag kennis van nemen en in de gelegenheid worden gesteld om hier haar zienswijze op te geven. In het verleden heeft T-Mobile regelmatig in een juridische spagaat gestaan als het ging om het naleven van haar wettelijke verplichtingen ten aanzien van enerzijds het verstrekken van informatie aan opsporingsdiensten en anderzijds het naleven van privacywetgeving. Een herhaling van zetten dient voorkomen te worden, consistentie en transparantie ten aanzien van wetgeving is ons inziens dan ook een noodzaak.

Kosten

Ook de belangen van het bedrijfsleven mogen niet onbesproken gelaten worden. Zoals de wet nu is opgesteld zullen de kosten grotendeels op de bedrijven worden afgewenteld. De in de Memorie van Toelichting neergelegde verwijzing (artikel 32 lid 8) naar artikel 13.6 van de Telecommunicatiewet verwijst naar een vergoeding ten aanzien van administratie en personeelskosten. Gesteld wordt dat: "*Er bestaat geen aanleiding om voor deze aanbieders een (deels) afwijkende regeling te treffen*".
Hierbij wordt door uw ministerie volledig voorbijgegaan aan de investerings-, exploitatie- en onderhoudskosten welke marktpartijen zullen moeten doen, willen ze kunnen voldoen aan de verplichtingen zoals gesteld in het wetsvoorstel. Door de door uw ministerie geïntroduceerde verplichtingen ten behoeve van de uitvoering van de wet, ontstaat voor de betrokken telecomaanbieders, disproportionele en niet te billijken verplichtingen.

In haar huidige bedrijfsvoeringen en dienstverlening naar haar klanten toe heeft T-Mobile de informatie die de diensten vraagt niet nodig. De kosten die hiervoor gemaakt moeten worden dienen dan ook niet voor rekening van T-Mobile te komen.

Ervaring leert ons dat om gevallen van ongelimiteerde en onnodige aanvragen te voorkomen, het instellen van een extra toets-moment voorafgaand aan de op te vragen informatie gewenst is.
In de Memorie van Toelichting, pagina 201/202 Hoofdstuk 10, wordt aangegeven dat er op dit moment nog geen gedetailleerd inzicht in de kosten van interceptie kan worden gegeven en dat deze kosten in nauw overleg met de relevante telecomaanbieders in kaart moeten worden gebracht.
Aannemende dat T-Mobile gezien wordt als een relevante telecomaanbieder valt de tekst op dezelfde pagina op: '*Mede om ervaring op te doen op grond waarvan gerichte vervolgstappen kunnen worden genomen, zal de interceptie na inwerkingtreding van de wet in de aanvangsjaren tot enkele fysieke toegangspunten beperkt blijven*'. Deze tekst geeft ons de indruk dat de aanbieders 'cursussen' moeten gaan aanbieden om de kennis van de diensten te vergroten en continue kostbare investeringen moet gaan doen in de interceptie omgeving, zonder dat de diensten gelimiteerd worden. Met dit wetsvoorstel lijken de diensten een carte blanche te krijgen als het gaat om het product protfolio voór interceptie

zonder voorafgaande wettelijke toetsingsmomenten. Dit kan ons inziens nooit de bedoeling zijn van het onderhavige wetsvoorstel en is voor T-Mobile ook niet acceptabel.

Netwerk

In het voorstel staat weergegeven dat de diensten bevoegd zijn tot het verkennen van geautomatiseerde werken die op ons (T-Mobile) netwerk zijn aangesloten (artikel 30 sub a) en daarvoor gebruik kunnen maken van technische voorzieningen. Het risico is aanwezig dat hierdoor ons netwerk aanpassingen kan ondergaan die ontregelend kunnen zijn voor het functioneren van het netwerk, bijvoorbeeld door de inzet van IMSI catchers of het inzetten van probes op ons netwerk. Dit zou behalve voor een slechte performance van ons netwerk, met bijbehorende imagoschade, er tevens voor kunnen zorgen dat T-Mobile buiten haar wil (en buiten haar bereik) niet voldoet aan de aan haar opgelegde wetgeving uit de Telecommunicatiewet en de Wet bescherming persoonsgegevens. Hierbij moet gedacht worden aan zorgplichten als privacy en continuïteit.
T-Mobile zou graag van u vernemen welke passende maatregelen zullen worden genomen en hoe dergelijke potentiele problemen voorkomen gaan worden.

Artikel 33 lid 1 en de bijbehorende passage uit de Memorie van Toelichting op pagina 71, geeft aan dat de dienst DPI toe gaat passen om dataverkeer te analyseren. Wat niet duidelijk wordt uit de tekst is wie deze dienst gaat toe passen. Zijn dit de diensten zelf of is dit de netwerkaanbieder?

Europa

In artikel 76 van het wetsvoorstel wordt aangegeven dat de diensten bevoegd zijn tot het aangaan van samenwerkingsrelaties met andere landen (lid 1). Deze samenwerking wordt gewogen volgens de criteria die in lid 3 zijn opgenomen. Deze criteria worden gezien als minimum criteria. Het gaat om democratische inbedding (a), eerbiediging van mensenrechten (b) en professionaliteit en betrouwbaarheid (c) van het betreffende land. Dit lijken ook niet meer dan logische criteria, maar wel marginaal en moeilijk aantoonbaar. Er wordt ook niet aangegeven op welke manier de criteria worden getoetst door de dienst.
Voor T-Mobile is het van essentieel belang, en stelt daarom ook de vraag, op welke manier de (bedrijfs)vertrouwelijke informatie wordt beschermd (opslag en verzending) en wat er gebeurt indien deze vertrouwelijke informatie op straat komt te liggen. Wie zal hiervoor de verantwoording op zich nemen?

Encryptie

Encryptie van dataverkeer, zowel van data in transit als van opgeslagen data, maakt grootschalige onderschepping van data door inlichtingen- en veiligheidsdiensten niet alleen veel moeilijker, maar ook veel duurder.
Het wetsvoorstel geeft de mogelijkheid om een aanbieder te dwingen de communicatie te decrypten, De medewerkingsverplichting is in artikel 132 zelfs strafbaar gesteld.
Decryptie is echter in veel gevallen niet mogelijk door onder andere het ontbreken van de sleutels. Het wordt in de tekst en artikelen niet duidelijk hoever de medewerkingsverplichting reikt. Kan de decryptie-

verplichting ook inhouden "het in het netwerk inbouwen van gedeeltelijk uitschakeling van encryptiemethoden"?

Termijnen

Het wetsvoorstel geeft in meerdere artikelen bewaartermijnen aan van relevante en irrelevante data onder dat hier enige onderbouwing aan ten grondslag ligt. Opmerkelijk omdat eerdere wetgeving over bewaartermijnen in de "Wet bewaarplicht telecommunicatie gegevens" mede om die reden buiten werking is gesteld.
Soms is het niet duidelijk hoe lang data (mogen) worden bewaard; in artikel 33 lid 5 staat aangegeven dat gegevens ten hoogste drie maanden worden bewaard, echter in de tweede zin van het artikel wordt aangegeven dat na deze periode niet relevante gegevens worden vernietigd. Dit impliceert dat relevante gegevens langer worden bewaard. Nergens wordt duidelijk hoelang de bewaartermijn maximaal kan zijn.

Uiteraard gaan wij graag met U en uw collega's in gesprek over onderhavige voorgenomen wetswijziging.

Met vriendelijke groeten,
namens T-Mobile Netherlands B.V.

Joepke van der Linden
Sr. Regulatory Affairs Counsel

BCPA

Ministerie van Binnenlandse Zaken
en Koninkrijksrelaties

Amsterdam, 31 augustus 2015

Betreft: *Consultatie Wet op de inlichtingen- en veiligheidsdiensten 20..*

Geachte dames en heren,

Hierbij reageert BCPA op het concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX (consultatieversie juni 2015).

Inleiding

BCPA is een samenwerkingsverband van de in Nederland actieve dochterondernemingen van BT Group, Verizon Enterprise Solutions en Colt Technology Services. Deze aanbieders leveren wereldwijd telecommunicatiediensten en IT-oplossingen aan grootzakelijke klanten en overheidsinstellingen.

BCPA volstaat in deze zienswijze met een kritische reactie op het voorstel om aanbieders van communicatiediensten te verplichten om mee te werken aan ongerichte interceptie in 'bulk' (artikel 33 en artikel 37). Deze verplichting is niet noodzakelijk, niet proportioneel en niet duidelijk. Ten onrechte worden aanbieders niet gecompenseerd voor hun investeringen. BCPA licht dit standpunt hierna toe.

Verplichting is onvoldoende duidelijk bepaald

De bevoegdheid om verkeer in 'bulk' te onderscheppen is bijzonder ruim omschreven. Hetzelfde geldt voor de corresponderende medewerkingsverplichting. Noch in de wet noch in de Memorie van Toelichting is omschreven wat de medewerkingsplicht voor aanbieders precies behelst. De bevoegdheid wordt op geen enkele wijze begrensd.

De Memorie van Toelichting vermeldt slechts dat 'maatwerk is vereist', en dat de diensten een 'nauwkeurige omschrijving' moeten geven van de soort medewerking welke van de aanbieder wordt verlangd. De voorzieningen die moeten worden getroffen zijn niet beschreven, laat staan gespecificeerd. Een en ander moet worden uitgewerkt in nader overleg met de aanbieders.

Lasten voor het bedrijfsleven: blanco cheque

Uit het wetsvoorstel blijkt niet dat is nagedacht over de lasten voor het bedrijfsleven. De lasten voor het bedrijfsleven worden nergens beschreven, ook niet in hoofdstuk 11 van de Memorie van Toelichting, dat is gewijd aan de lasten voor het bedrijfsleven.

Wanneer de aanbieders de kosten voor hun rekening moeten nemen is het des te meer van belang dat de verplichting duidelijk en begrensd is. Dat is niet het geval. Aanbieders worden in feite geacht om een blanco cheque uit te schrijven. BCPA maakt hier bezwaar tegen. Aanbieders moeten redelijkerwijs in staat zijn om een begroting op te stellen en om de benodigde projectwerkzaamheden in te plannen.

Regeling is niet noodzakelijk en niet proportioneel

Het maatschappelijk belang van misdaad- en terrorismebestrijding is evident. Niettemin moet de vraag worden gesteld in hoeverre nieuwe bevoegdheden en verplichtingen noodzakelijk en proportioneel zijn. De noodzaak van de nieuwe bevoegdheid is niet evident. Iedere onderbouwing ontbreekt in het voorstel. De regeling is ook niet proportioneel, om twee redenen.

Ten eerste worden, als gezegd, aanbieders geacht om een blanco cheque uit te schrijven. Dit maakt de regeling evident disproportioneel. Ten tweede is het niet proportioneel om deze verplichting aan alle aanbieders op te leggen. Grootzakelijke aanbieders, zoals BT, Colt en Verizon, zijn vanwege de aard van hun dienstverlening niet of nauwelijks in staat om bij te dragen aan de bestrijding van de misdaad en bij het handhaven van de staatsveiligheid. Toch zullen ook zij volop moeten investeren om te voldoen aan de nieuwe verplichtingen.

Zoals steeds het geval is bij wetgeving inzake bevoegd aftappen en data-retentie ontbreekt zelfs een summiere kosten-batenanalyse. BCPA maakt hier opnieuw bezwaar tegen. Het is niet bij voorbaat redelijk om de kosten die zijn gemoeid met het dienen van een maatschappelijk belang neer te laten slaan bij telecomaanbieders. En zeker niet bij grootzakelijke aanbieders, die geen diensten leveren die gewoonlijk door criminelen of terroristen worden afgenomen.

Vrijstelling

BCPA heeft bij herhaling gepleit voor een vrijstelling van aftap- en bewaarverplichtingen voor aanbieders die niet of nauwelijks worden bevraagd. Als voorbeeld noemt BCPA de vrijstelling van de bewaarplicht die geldt in het Verenigd Koninkrijk. Aanbieders die minder dan 10.000 klanten bedienen worden in het Verenigd Koninkrijk in beginsel niet aangewezen om te voldoen aan de bewaarplicht. Aanbieders die wel worden aangewezen ontvangen een vergoeding voor hun medewerking. Behoeftestellers betrekken dus de kosten in hun afweging. Dit maakt dat behoeftestellers per definitie oog hebben voor de noodzakelijkheid en proportionaliteit van een maatregel. Deze systematiek verdient navolging.

Grensoverschrijdende werking

BCPA noemt nog een laatste bezwaar. De verplichting heeft betrekking op al het verkeer dat via de netwerken van in Nederland gevestigde aanbieders wordt afgehandeld, ook op verkeer tussen niet in Nederland gevestigde klanten, dat om technische redenen (deels) via een Nederlands netwerk wordt afgehandeld. De verkregen informatie kan bovendien worden uitgewisseld met inlichtingen- een veiligheidsdiensten uit andere landen (artikel 49 en 77). Deze bijzonder ruime, grensoverschrijdende bevoegdheden zullen afbreuk doen aan de aantrekkingskracht van Nederland als vestigingsland voor bedrijven voor internationaal opererende telecomaanbieders en hun klanten. Deze bevoegdheden staan bovendien haaks op het streven naar een digitale eengemaakte Europese markt.

Conclusie

De noodzaak om op grote schaal ongericht in 'bulk' verkeer te onderscheppen is niet gegeven, en wordt in het voorstel niet aangetoond. De financiële consequenties zijn even onduidelijk als verstrekkend. Dit is met name onbillijk ten aanzien van aanbieders die niet of nauwelijks kunnen bijdragen aan de opsporing van strafbare feiten en aan het handhaven van de staatsveiligheid. Een vrijstelling voor zulke aanbieders ligt in de rede.

De plannen zijn kritisch ontvangen in de pers, en een record aantal zienswijzen is inmiddels ingediend via internetconsultatie.nl. BCPA wijst in het bijzonder op de zienswijze van het Instituut voor Informatierecht, verbonden aan de Faculteit der Rechtsgeleerdheid van de Universiteit van Amsterdam (IViR). Het IViR concludeert dat het wetsvoorstel niet voldoet aan de standaarden die zijn gebaseerd op grondrechtelijke verplichtingen. Mocht dit wetsvoorstel ongewijzigd worden aangenomen, dan dreigt herhaling van het bewaarplichtscenario, met alle kosten van dien.

BCPA is desgewenst graag bereid om deze zienswijze nader toe te lichten.

VNO NCW

MKB Nederland

Zijne Excellentie
dr. R.H.A. Plasterk
Minister van Binnenlandse Zaken en
Koninkrijksrelaties
Turfmarkt 147
2511 DP DEN HAAG

Briefnummer
15/11.160/Ma/Man

Onderwerp
Wetsvoorstel WIV

Den Haag
31 augustus 2015

Telefoonnummer
070-3490352
E-mail
mallens@vnoncw-mkb.nl

Excellentie,

Op 2 juli 2015 heeft u het wetsvoorstel Wet op de Inlichtingen- en veiligheidsdiensten 20.. (WIV) ter consultatie voorgelegd. VNO-NCW en MKB-Nederland waarderen de geboden mogelijkheid om hun zienswijze op het wetsvoorstel te geven.
In brede zin zijn VNO-NCW en MKB-Nederland van mening dat de inlichtingen- en veiligheidsdiensten over voldoende bevoegdheden dienen te beschikken om hun taken op een effectieve manier te kunnen uitoefenen. Zij vragen zich echter af of de in dit wetsvoorstel voorziene vergaande uitbreiding van de bevoegdheden van de diensten in alle gevallen noodzakelijk en proportioneel is.

Maatvoering is essentieel om enerzijds de belangen in het kader van de nationale veiligheid te beschermen, maar tegelijkertijd de belangen van de betreffende ondernemingen, personen en in het algemeen ons investeringsklimaat te borgen. Het gaat dan onder meer om maatvoering in de reikwijdte van de bevoegdheden (wie vallen onder de wet, wat mag van een bedrijf gevraagd worden) en maatvoering in kosten (deze mogen niet grotendeels op het bedrijfsleven worden afgewenteld). Daarbij zullen risico's voor bedrijven, zoals aansprakelijkheid jegens gebruikers of verlies van bedrijfsgevoelige informatie, zoveel mogelijk beperkt moeten worden.

Specifiek levert de wijziging van de wet de volgende vragen en opmerkingen op:

- De in dit wetsvoorstel voorziene uitbreiding van de bijzondere bevoegdheid van de diensten om 'in bulk' het kabelgebonden verkeer af te tappen is verregaand.

De enkele constatering dat tegenwoordig verreweg het grootste deel van de communicatie via kabelnetwerken verloopt, vormt naar onze mening hiervoor onvoldoende rechtvaardiging. De huidige, gerichte internettap biedt ons inziens voldoende mogelijkheden voor de diensten om hun taken te kunnen uitvoeren. Wij vragen de minister dan ook om een onderbouwing van nut, noodzaak én effectiviteit van deze vergaande aanpassingen.

- VNO-NCW en MKB-Nederland zijn bezorgd over de effecten die deze wetgeving zal hebben op het investeringsklimaat in Nederland, in het bijzonder voor de internettechnologiesector. De Nederlandse digitale infrastructuur en de bedrijvigheid die dit met zich mee brengt, zijn van groot belang voor onze economie. De betekenis van het huidige voorstel op het vereiste vertrouwen van bedrijven om online te communiceren en zaken te doen is onvoldoende onderzocht.

- Risico voor ondernemingen is dat bedrijfsvertrouwelijke informatie waaronder economisch waardevolle intellectuele eigendom weglekt. Naast openbare telecommunicatienetwerken kunnen ook aanbieders van overige communicatiediensten worden gedwongen om mee te werken aan de uitvoering van een toestemming tot aftappen of opnemen van telecommunicatie die over de telecomnetwerken wordt afgewikkeld. Ingevolge artikel 77, lid 2 kan afgetapte informatie vervolgens aan derden (andere inlichtingendiensten) worden doorgegeven. Graag vernemen wij van de minister welke garanties het wetsvoorstel biedt om het weglekken van bedrijfsvertrouwelijke informatie te voorkomen.

- Een ander risico is dat de diensten nieuwe bevoegdheden krijgen om bepaalde technische voorzieningen aan te brengen. Het risico bestaat dat daarmee ook geautomatiseerde werken van derden (zoals telecom aanbieders) aanpassingen kunnen ondergaan die hen buiten hun wil en buiten hun macht strafbaar maken vanuit verschillende zorgplichten (privacy, cybersecurity).

  Een ander niet uit te sluiten risico is dat andere partijen de 'voorzieningen' gaan misbruiken die de diensten hebben aangelegd, waarbij de betrokken aanbieder als schuldige wordt aangemerkt, met alle wettelijke gevolgen van dien, denk aan vervolging of aansprakelijkstelling. Zelfs als de aanbieder op de hoogte is van de voorzieningen verlet de geheimhoudingsplicht van aanbieder om zich effectief te verdedigen.

- De verplichting voor ondernemingen om mee te werken aan de ontsleuteling van communicatie en gegevens en/of het opleveren van sleutels brengt de ondernemingen in een lastig parket. Allereerst is het vrijmaken van sleutels voor transport veelal onmogelijk omdat die sessie-gebonden en vluchtig zijn. Of zij zijn hardwarematig beschermd waardoor vrijmaken tot netwerkuitval zal leiden met alle consequenties van dien.

De verplichte medewerking aan ontsleuteling en/of het opleveren van sleutels brengt aanbieders bovendien in direct conflict met de privacy- en cybersecurityzorgplicht die de onderneming jegens de gebruiker heeft.

- Belangrijk zorgpunt is voorts dat de kosten van uitvoering van dit wetsvoorstel vrijwel volledig bij het bedrijfsleven worden gelegd. De zeer beperkte vergoedingsregeling uit het Besluit aftappen openbare Telecommunicatienetwerken en -diensten wordt onverkort van overeenkomstige toepassing verklaard op alle aanbieders van een dienst die over het internet gegevens uitwisselt.
  Met deze ruim geformuleerde wetteksten is er alle vrijheid zeer veeleisende en vaak kostbare medewerking (consultancy) te claimen zonder dekkende financiële compensatie.
  Wij dringen er bij u op aan in elk geval eerst via een bedrijfseffectentoets de lasten voor het bedrijfsleven te (laten) berekenen alvorens het voorstel naar de Ministerraad wordt gestuurd.

  Aangezien de diensten hun taken uitoefenen in het kader van de bescherming van de nationale veiligheid, hetgeen bij uitstek een overheidstaak is, moeten de kosten van uitvoering van dit wetsvoorstel ons inziens ook voor rekening van de overheid komen. Dit kan ook bijdragen aan het voorkomen van een te snelle inzet van vergaande bijzondere bevoegdheden.

  Recentelijk is bij de behandeling van het wetsvoorstel Wet Veiligheidsonderzoeken in de Eerste Kamer gesproken over het vraagstuk van het doorberekenen aan bedrijven van kosten van handelingen en diensten in het kader van de uitvoering van een overheidstaak. In dit verband roepen wij in herinnering uw toezegging aan de Eerste Kamer om hierover een bestendige beleidslijn, inclusief een afwegingskader, te ontwikkelen.

Mocht u naar aanleiding van deze opmerkingen nog vragen hebben, dan zijn wij natuurlijk graag bereid een nadere toelichting te geven.

Hoogachtend,

drs. C. Oudshoorn
directeur beleid

Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX: een respons van Internet Society Nederland op de consultatieversie juni 2015

Amsterdam, 28 augustus 2015

Internet Society Nederland
bureau@isoc.nl

www.isoc.nl

Over ISOC Nederland

Internet voor iedereen

De Internet Society (ISOC) streeft naar een open, neutraal, gedecentraliseerd en voor iedereen toegankelijk en betrouwbaar internet. ISOC maakt zich sterk voor globale samenwerking op het gebied van internet- en gerelateerde technologieën: ISOC is de moederorganisatie voor een aantal toonaangevende internationale organen die zich bezig houden met het ontwikkelen en bevorderen van het gebruik van open internetstandaarden en -protocollen. Denk aan de Internet Engineering Task Force (IETF), de Internet Architecture Board (IAB), en de Internet Engineering Steering Group (IESG.

Daarnaast is ISOC pleitbezorger van een brede maatschappelijke discussie over internet-gerelateerde onderwerpen waarbij alle belanghebbenden evenredig vertegenwoordigd dienen te zijn.

In dat kader is één van de 'core values' van ISOC is bij uitstek relevant in deze respons :[1]

> 'The social, political, and economic benefits of the Internet are substantially diminished by excessively restrictive governmental or private controls on computer hardware or software, telecommunications infrastructure, or Internet content.'

ISOC is erkend door de Verenigde Naties en actief in 170 landen. Onder het motto 'het internet is voor iedereen' zet ISOC zich onder andere in voor de bevordering van wet- en regelgeving die de verdere ontwikkeling van het grenzeloze internet mogelijk maakt.

Internet Society Nederland is de Nederlandse afdeling ('chapter') van ISOC en als zodanig onderdeel van deze internationale niet-gouvernementele organisatie. Deze respons is echter ingediend namens ISOC Nederland en niet ISOC internationaal.

[1] http://www.internetsociety.org/who-we-are/mission/values-and-principles

Inleiding

Op 2 juli jl. is het wetsvoorstel om de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) aan te passen ter consultatie gepubliceerd.[2] Uiterlijk 1 september kan een ieder reageren op deze kabinetsvoornemens alvorens het concept, al dan niet aangepast naar aanleiding van de respons op de consultatie, naar de Raad van State gaat. Bij deze maakt Internet Society Nederland (ISOC Nederland) een aantal fundamentele zorgen die zij heeft met betrekking tot het wetsvoorstel kenbaar.

Aanpassing bijzondere bevoegdheden van de diensten: interceptie van kabelgebonden telecommunicatie in 'bulk'

Het Kabinet neemt in de 218 pagina's aan Memorie van Toelichting (MvT) bij het wetsvoorstel de conclusies en aanbevelingen uit het Wiv 2002 evaluatierapport van de commissie Dessens [3] 'in algemene zin' over. 'Inhoudelijk is de regeling inzake de verwerking van gegevens door de diensten op diverse onderdelen ingrijpend gewijzigd, met name waar het gaat om de bijzondere bevoegdheden van de diensten', aldus bladzijde 20 van de MvT. En inderdaad, zoals verwacht, op pagina 55 staat dat 'deze bevoegdheden thans technologieonafhankelijk (worden) geformuleerd, waarmee de bestaande beperking tot niet-kabelgebonden telecommunicatie komt te vervallen en derhalve ook kabelgebonden telecommunicatie voor interceptie als hier bedoeld (interceptie in "bulk") in aanmerking komt.'

Er valt wellicht iets voor te zeggen het onderscheid tussen media te laten 'vervallen' vanwege 'technologische ontwikkelingen'[4], maar waarom dan niet de huidige, beperktere kabelgebonden bevoegdheden naar het draadloze domein vertalen in plaats van andersom zoals nu gebeurt? De intentie van het Kabinet met betrekking tot 'kabelgebonden telecommunicatie' is echter heel helder: het gaat om beoogde '*interceptie in "bulk"*'.

Pagina 63 van de MvT zegt dat 'naast een explosieve groei van de hoeveelheid gegevens die in de wereld wordt geproduceerd (en elke twee tot drie jaar verdubbelt) moet worden vastgesteld dat inmiddels ongeveer 90% van alle telecommunicatie via kabelnetwerken verloopt. In de huidige wet is met deze ontwikkeling geen rekening gehouden.' En 'om zicht te houden op de dreigingen zijn de diensten afhankelijk van een adequate toegang tot telecommunicatie. (...) Bijzondere bevoegdheden die het mogelijk maken om – onder strikte

---

[2] http://www.internetconsultatie.nl/wiv

[3] http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2013/12/02/rapport-evaluatie-wiv-2002.html

[4] Alhoewel: bij interceptie in het publieke (!) draadloze domein vindt geen schending plaats van de integriteit van apparatuur en/of infrastructuur van een derde. Dat staat ook in zoveel woorden in de MvT op blz 203: 'De huidige wet kent in artikel 27 de bevoegdheid tot ongerichte interceptie van niet-kabelgebonden telecommunicatie, waarbij niet voorzien is in een medewerkingsplicht voor aanbieders van een openbaar telecommunicatienetwerk of openbare telecommunicatiedienst.' Die medewerkingsplicht is namelijk niet vereist om ongericht niet-kabelgebonden telecommunicatie te intercepteren. Daarnaast kan men betogen dat gebruikers van e.g. satellietcommunicatievoorzieningen een duidelijker en in ieder geval beperktere doelgroep vormen. Noodzakelijkheid en proportionaliteit van inzet van bijzondere bevoegdheden zijn in dat geval beter te beargumenteren.

voorwaarden – in bulk te intercepteren in het kabelgebonden domein zijn daarbij onmisbaar.'

Oftewel ongericht, in 'bulk via de 'kabel' want 'onmisbaar', en noodzakelijk en proportioneel. Aldus het Kabinet.

Nut en Noodzaak

Op basis van de stukken is ISOC Nederland er echter geenszins van overtuigd dat genoemde noodzakelijkheid is aangetoond en dat deze vervolgens opweegt tegen de potentieel ernstige inbreuk op de persoonlijke levenssfeer van privépersonen, zoals het Kabinet overigens zelf ook vaststelt.

Nederland behoort tot de top in de wereld als het gaat om gebruik van breedband- en mobiel internet door haar burgers, en beschikt over een zeer geavanceerde open en neutrale internetinfrastructuur. Wat betekent de inzet van de nieuwe bijzondere bevoegdheden voor het vereiste vertrouwen van personen, bedrijven en andere organisaties om online te communiceren en zaken te doen in Nederland? Wat zijn de economische consequenties? Dat laatste element ontbreekt geheel in de motivatie van het Kabinet.[5] Terwijl de onthullingen van Snowden over het gedrag van Amerikaanse veiligheidsdiensten er wel degelijk voor gezorgd hebben dat online bedrijvigheid uit de Verenigde Staten verdween.[6]

Voordat het instrumentarium van de diensten uitgebreid wordt zoals voorgesteld, moet volgens ISOC Nederland allereerst grondig en vooral onafhankelijk onderzoek plaatsvinden naar de effectiviteit, en dus proportionaliteit, van ruimere bevoegdheden en het ongericht kunnen tappen op kabelgebonden infrastructuur. Uit studies in andere landen blijkt deze op zijn minst twijfelachtig.[7] Politieke prioriteit en gebrek aan transparantie staat dan hoger op de agenda dan (on)gewenst resultaat. Hoeveel veiliger wordt de situatie? Welke aanslagen zijn daadwerkelijk en aantoonbaar vermeden? Hoe kunnen we beoordelen of geïmplementeerde maatregelen de beoogde (welke?) resultaten realiseren en of deze inderdaad opwegen tegen de 'collateral

---

[5] Zeer opmerkelijk gezien de al in 2011 gestelde ambities van het Kabinet om van Nederland een 'Digital Gateway to Europe' te maken. Zie de Digitale Agenda http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/notas/2011/05/17/digitale-agenda-nl-ict-voor-innovatie-en-economische-groei/282931-e07-digitale-agenda.pdf, en ook de https://digitale-infrastructuur.nl/ rapporten uit 2013 en 2014. Het economische belang van de Nederlandse digitale infrastructuur wordt inmiddels door een ieder erkend: het is een essentiële en snel groeiende 'third mainport', naast de haven van Rotterdam en Schiphol.

[6] http://www2.itif.org/2013-cloud-computing-costs.pdf

[7] Zie het 'Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court' van de Amerikaanse 'Privacy and Civil Liberties Oversight Board https://www.documentcloud.org/documents/1008957-final-report.html op blz 11: 'We have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack.'

damage'? Er zal toch op zijn minst in concreet onderbouwde termen aannemelijk gemaakt moeten worden dat bestaande bevoegdheden ontoereikend zijn.

Ook de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) stelt in haar jaarverslag 2014-2015 dat:[8]

'De Commissie het als een gemis (ervaart) dat in Nederland vooralsnog nauwelijks wordt gediscussieerd over *de vraag in hoeverre het noodzakelijk is bevoegdheden uit te breiden*. De nadruk in de discussies ligt al snel op de rechtmatigheid van het handelen en minder op de doelmatigheid of effectiviteit van interceptiebevoegdheden. *De discussie kan daardoor blijven hangen bij de constatering dat tegenwoordig 90 procent van de communicatie over de kabel gaat en daardoor de 'traditionele' bevoegdheid tot het ongericht intercepteren van satellietcommunicatie (de resterende 10 procent) niet meer volstaat. Maar kan deze constatering alleen de conclusie tot de uitbreiding van de bevoegdheden dragen? Daarvoor moet men toch een beeld hebben van de effectiviteit en/of het gebrek daaraan van de bestaande bevoegdheden?* Ook internationaal is dit een vraag die de gemoederen bezighoudt, maar waarover weinig uitsluitsel wordt gegeven. *Uitgangspunt zou moeten zijn dat eerst de noodzaak voor nieuwe bevoegdheden, ingegeven door tekortschietende effecten van de huidige bevoegdheden, overtuigend moet worden aangetoond voordat sprake kan zijn van een wettelijke uitbreiding.*'

En daar voegt de CTIVD aan toe:

'*Deze effectiviteitstoets wordt ook ingegeven door de rechtmatigheidstoets die artikel 8 van het Europees Verdrag voor de Rechten van de Mens voorschrijft vanuit het oogpunt van privacybescherming. Daarbij staat niet alleen ter beoordeling welke schade aan de nationale veiligheid wordt voorkomen, maar tevens welk nadeel individuen wordt berokkend met de interceptiebevoegdheden.*'

(cursivering en onderstreping door ISOC Nederland)

Integraal Afwegingskader?

Het is aan het Kabinet om nut en noodzaak van het wetsvoorstel aan te tonen, niet aan derden om aan te geven hoe deze onderbouwing er uit moet zien. Het officiële 'Integraal Afwegingskader' (IAK)[9] kan in deze assistentie verlenen.

'Het IAK is een werkwijze en informatiebron en toe te passen op elk moment in het beleidsproces. Met name in een vroeg stadium van het beleidsproces heeft de toepassing van het IAK meerwaarde. Elk voorstel voor beleid of regelgeving dat wordt voorgelegd aan het parlement moet een adequaat antwoord bevatten op de 7 hoofdvragen van het IAK:

1. Wat is de aanleiding?
2. Wie zijn betrokken?
3. Wat is het probleem?

---

[8] http://www.ctivd.nl/documenten/jaarverslagen/2014/04/30/jaarverslag-2014 , blz 28

[9] https://www.kcwj.nl/kennisbank/integraal-afwegingskader-beleid-en-regelgeving

4. Wat is het doel?
5. Wat rechtvaardigt overheidsinterventie?
6. Wat is het beste instrument?
7. Wat zijn de gevolgen?'

ISOC Nederland heeft sterk de indruk dat de 'verplichte kwaliteitseisen' waarop het IAK is gebaseerd, niet zijn meegenomen bij de totstandkoming van het wetsvoorstel:[10]

Veiligheidsbewustzijn van targets en hacken van onschuldige technisch zwakkere randgebruikers

De MvT wijst op het 'veiligheidsbewustzijn' van 'targets', en knoopt daar vervolgens een wat ISOC Nederland betreft perverse conclusie aan op blz. 53 dat dit 'kansen' biedt 'tot het benutten van zwakheden bij technische randgebruikers'. Gericht hacken via (apparatuur van) bij voorbaat niet-verdachten en onschuldigen, in de hoop dat men op deze wijze indirect bij de 'targets' kan komen. Zie artikel 30, eerste lid, onder b, van het wetsvoorstel. Los daarvan dient men zich in ieder geval af te vragen in hoeverre massale ongerichte interceptie een toegevoegde waarde levert in termen van het beschermen van nationale veiligheidsbelangen wanneer technisch onderlegde individuen en groepen de vertrouwelijkheid van hun communicatie relatief eenvoudig weten te waarborgen. Voor ISOC Nederland stellen anonimiteit en gebruik van encryptie burgers juist in staat hun recht op vrijheid van meningsuiting en expressie uit te oefenen. En ook in termen van het geven van een 'tegenmacht' richting het opereren van veiligheidsdiensten is ISOC Nederland van mening dat encryptie er voor zorgt dat de kosten van massasurveillance verhoogt worden en diensten dwingt interceptie specifiek te maken en te houden. Anonimiteit en gebruik van encryptie zouden dus vanuit overheidswege beschermd, geborgd en zelfs gepromoot moeten worden.[11] Daar gaan de kabinetsvoornemens echter rechtstreeks tegenin, een algemeen decryptiebevel incluis. Zie bijvoorbeeld artikel 30, lid 5 en 8, en artikel 41.

Effectiviteit bijzondere bevoegdheden

Een feit is daarnaast dat daders van recent gepleegde aanslagen in het buitenland al lang in beeld waren van diensten. Hoe effectief is dan één en ander? Is dit indicatief voor de beperkingen die te ruime bevoegdheden met zich brengen? Men is op zoek naar een speld in een hooiberg maar creëert de facto extra hooibergen. Hoe dan ook, dit soort vragen verdient een fundamentele

---

[10] https://www.kcwj.nl/kennisbank/integraal-afwegingskader-beleid-en-regelgeving/verplichte-kwaliteitseisen : 'Het IAK is gebaseerd op de verplichte kwaliteitseisen, die de ministerraad op 14 april 2011 heeft vastgesteld.

[11] Zie rapport UN rapporteur Freedom of Expression David Kaye 'on the promotion and protection of the right to freedom of opinion and expression van 22 mei 2015 http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc : 'With respect to encryption and anonymity, States should adopt policies of non-restriction or comprehensive protection, only adopt restrictions on a case-specific basis and that meet the requirements of legality, necessity, proportionality and legitimacy in objective, (and) require court orders for any specific limitation' en 'states should not restrict encryption and anonymity, which facilitate and often enable the rights to freedom of opinion and expression'

discussie op basis van onafhankelijk gepresenteerd feitenmateriaal. Zolang dat er niet is, en de effectiviteit van nieuwe bevoegdheden dus niet ingeschat kan worden, is uitbreiding van bevoegdheden bij voorbaat niet noodzakelijk en -proportioneel.

Grondrechten van burgers

Het Kabinet lijkt zich bewust dat 'de uitoefening van deze bijzondere bevoegdheden per definitie raakt aan het recht op bescherming van privacy van de burgers.'[12] Echter, 'gelet op de verantwoordelijkheid en de zorg van de overheid voor de veiligheid van haar burgers is het onontkoombaar dat de diensten persoonsgegevens verzamelen en verwerken.' Sterker nog, 'de overheid beoogt met gepaste en doelgerichte uitoefening van deze bevoegdheden bij te dragen aan het realiseren in een veilige samenleving van grondrechten, waaronder ook het recht op privacy.' De uitbreiding van de bevoegdheden moet er dus komen omdat deze (o.a.) bijdraagt aan de bescherming van het recht op privacy? Dat klinkt voor ISOC Nederland als een drogreden...

Ook in de MvT wordt meerdere keren aan het aspect van (de inbreuk op) grond- en mensenrechten gerefereerd. In hoofdstuk 1 staat bijvoorbeeld:

'Diverse in het wetsvoorstel opgenomen bepalingen inzake de verwerking van gegevens, waarbij naast de algemene bevoegdheid tot gegevensverzameling ook bijzondere bevoegdheden ter zake kunnen worden ingezet, maken – in meer of mindere mate – een inbreuk op relevante grond- en mensenrechten, in het bijzonder de artikelen 10, 12 en 13 Grondwet en artikel 8 EVRM. Bij de uitwerking van de verschillende bevoegdheden en andere relevante aspecten van gegevensverwerking (zoals de verstrekking van gegevens) is op de daaruit voortvloeiende eisen acht geslagen, waarbij op een evenwichtige manier recht is gedaan aan zowel het belang van de nationale veiligheid als aan dat van het recht op bescherming van de persoonlijke levenssfeer.'

In combinatie met het weinig steekhoudende pleidooi dat ongerichte interceptie beoogt 'bij te dragen aan het realiseren in een veilige samenleving van grondrechten', vindt ISOC Nederland niet dat in het voorstel 'op een evenwichtige manier recht is gedaan' aan de bescherming van die grondrechten. Gezien de intenties van het Kabinet ('interceptie in "bulk") mag men terdege rekening houden met een zekere vooringenomenheid in deze. Mede in een context van recente uitspraken door het Hof van Justitie van de Europese Unie[13] en de Haagse Rechtbank[14] zou ISOC Nederland onderbouwing willen zien door een onafhankelijke en deskundige partij hoe de voornemens zich (niet) verhouden tot e.g. een artikel 8 van het Europees Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (EVRM).[15] Alvorens tot

---

[12] Kamerstukken II 2013/14, 33 820, nr. 4.

[13] http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054nl.pdf
[14] http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2015:2498
[15] Als het gaat om vereist toezicht en bijbehorende transparantie, dan geeft IVIR daar een goede aanzet toe met een op 23 juli jl. gepubliceerd rapport http://www.ivir.nl/nieuws/tenstandards. Wat ISOC betreft neemt het Kabinet de erin opgenomen aanbevelingen één op één over.

een uitbreiding van bevoegdheden van diensten over te gaan[16].

Een pas op de plaats maken

ISOC Nederland is van mening dat er dus nog flink wat huiswerk is te doen: de uitgangspositie van het Kabinet is in de kern niet onderbouwd en gemotiveerd.

Het kan niet zo zijn dat vaag en eenzijdig gedefinieerde nationale veiligheidsbelangen de doorslag geven. Zoals Minister van Defensie Hennis-Plasschaert tijdens een Algemeen Overleg op 10 Februari jl. karikaturaal bevestigde [17]: de MIVD zou 'blind en doof' zijn. Ze noemde een aantal onduidelijke 'voorbeelden' die 'hoewel ik niet helemaal tot in detail kan gaan, er echt toe doen voor de informatiepositie van Nederland, de bescherming van de staatsveiligheid en onze belangen in het buitenland. Ik hoop dat ik daarmee de urgentie hiervan voor het voetlicht heb gebracht.' Oftewel noodzakelijk want 'urgent', volgens de Minister. Maar niet 'noodzakelijk' volgens ISOC Nederland. Men kan niet weg komen met het argument, zonder onderbouwing, dat openheid van zaken de 'informatiepositie van Nederland' schaadt. In een rechtstaat die Nederland pretendeert te zijn, moet als uitgangspunt gelden dat bijzondere bevoegdheden ook bijzondere verantwoording vereisen.

Een aantal specifieke elementen uit het wetsvoorstel

Er zijn vele elementen in het 83 bladzijden tellende wetsvoorstel die gedetailleerd aangevochten kunnen worden dan wel vragen oproepen, hetgeen volgens ISOC alleen maar bevestigt dat *eerst volstrekt helder moet gemaakt moet worden wat nut en noodzaak van de voorgestelde wijzigingen is.* Zoals het er nu staat is het voorstel buitenproportioneel. Er zal dus op zijn minst een pas op de plaats gemaakt moet worden. Enkele voorbeelden:

1. Toestemmingsvereisten

Toestemming voor de uitoefening van een bijzondere bevoegdheid door een dienst wordt verleend voor een periode van maximaal drie maanden, maar er is geen grens ('telkens') aan het aantal keren dat de toestemming verlengd kan worden, Aldus artikel 24 lid 3. Dat geldt ook voor interceptie 'in bulk' op de kabel. Die potentieel eindeloze tap is buitenproportioneel.

'Het nieuwe, technologieonafhankelijke stelsel voor de interceptie van telecommunicatie ("bulk") zal op hoofdlijnen uit een drietal fasen bestaan' Aldus de MvT op blz. 63: interceptie van data, voorbewerking van die data en 'verdere verwerking'. Voor ieder fase is een expliciete toestemming vereist. Echter de Minister kan ook een 'combinatie-last' geven, bijvoorbeeld gelijktijdig voor zowel

---

[16] Het Kabinet heeft na aandringen van de Tweede Kamer wel een 'privacy impact assesment' aangekondigd, 'parallel aan het in consultatie geven van het voorstel voor een nieuwe Wiv'. Aldus Minister Plasterk in een brief aan de Kamer van 17 maart jl (2015-0000158585). Ook de MvT refereert er aan in de titel van hoofdstuk 12: 'Hoofdstuk 12 Consultatie, adviezen en privacy impact assessment'. Het hoofdstuk zelf is echter leeg, en vooralsnog zijn doel, methode, tijdslijnen, en wat er met de resultaten gebeurt van genoemde voorgenomen 'assesment', volstrekt onduidelijk.

[17] http://www.tweedekamer.nl/vergaderingen/commissievergaderingen/details?id=2015A00163

fase 1 als 2. Hetgeen ook logisch klinkt want als men tot interceptie overgaat dan is dat natuurlijk enkel en alleen ten behoeve van de analyse van de inhoud van onderschepte data. Maar dit maakt de beoogde afbakening en de daarbij gesuggereerde controle wel minder expliciet en plausibel. Terwijl het Kabinet zelf aangeeft dat 'van fase tot fase derhalve in oplopende mate inzicht (wordt) verkregen in de persoonlijke levenssfeer. De waarborgen die in de wet zullen worden opgenomen, worden zwaarder naarmate de persoonlijke levenssfeer van individuen indringender in beeld komt'.[18] In de praktijk zal toestemming voor fase 1 dus het belangrijkst zijn voor de uitoefening van de analyse in fase 2 en 3.

Als de Minister besluit om toestemming te verlenen voor het uitoefenen van een bijzondere bevoegdheid door een dienst, dan kan de CTIVD, die daarvan op de hoogte gesteld wordt, aangeven wanneer zij van mening is dat die toestemming onterecht is. De Minister heeft dan een 'heroverwegingsplicht', maar kan het oordeel van de CTIVD desalniettemin naast zich neer leggen. Vervolgens is het aan de fractievoorzitters in de Tweede Kamer (de zo geheten 'commissie Stiekem') om te oordelen of de Minister al dan niet terecht het oordeel van de CTIVD naast zich neer heeft gelegd. De uiteindelijke beslissing komt dus niet bij een rechter of een onafhankelijke toezichthouder te liggen, maar bij politici. ISOC Nederland vindt het een zeer slechte zaak dat de toestemmingsvraag en het bijbehorende toezicht daarmee een fundamenteel politieke component hebben gekregen.[19]

2. Waarom uitzonderingen?

Waarom is er een uitzonderingspositie voor journalisten, waarbij in het kader van bronbescherming toetsing door rechter moet plaatsvinden (artikel 24 lid 4 van het wetsvoorstel) alvorens bijzondere bevoegdheden ingezet worden? Rechtelijke toetsing is natuurlijk prima, maar dat zou dan ook in alle andere gevallen zo moeten zijn. Terwijl dan toestemming van de Minister, of zelfs een aangewezen ambtenaar, toereikend is.

Artikel 29 stelt dat het briefgeheim ('het openen van brieven en andere geadresseerde zendingen, zonder goedvinden van de afzender of de geadresseerde') door diensten slechts te schenden is indien daartoe de rechtbank Den Haag een last heeft afgegeven. Waarom is dat ook niet zo bij andere, digitale vormen van communicatie, zoals email?[20] Daarnaast: het is toch

---

[18] Brief aan de Tweede Kamer 2014-0000622926, Kabinetsstandpunt herziening interceptiestelsel Wiv 2002, 21 november 2014

[19] Dit staat nog los van het ernstige feit dat het staatsgeheime informatie kan betreffen, en de Kamer bij een motie van wantrouwen, of zelfs in het uiterste geval bij het dwingen tot aftreden van een Minister, niet een publieke discussie kan voeren. En als het niet zover komt, en het Kabinet kan steunen op een meerderheid in de Tweede Kamer, dan mag men veronderstellen dat dit ook zo is in de 'Commissie Stiekem'. Hetgeen de oppositie in dat geval monddood maakt.

[20] Zie ook blz 195 van de MvT: 'Artikel 8 EVRM is niet alleen van toepassing op het brief-, telefoon- en telegraafgeheim, maar ook op inhoud van communicatie die via andere communicatiemiddelen wordt getransporteerd. Het thans aanhangig zijnde herzieningsvoorstel voor artikel 13 Grondwet stelt voor alle inhoud van communicatie, ongeacht met welk communicatiemiddel deze wordt overgebracht, aan dezelfde eisen te onderwerpen. Artikel 8 EVRM kent een hiermee vergelijkbare benadering. Artikel 8 EVRM vereist daarnaast dat een

de uitdrukkelijke intentie om de wet 'technologieonafhankelijk' te maken? Waarom dan een uitzondering voor 'brieven en andere geadresseerde zendingen'?

3. Hackbevoegdheid

Artikel 30 beschrijft het verkennen en binnendringen van geautomatiseerde werken inclusief een decryptiebevel (lid 5 en lid 8). Zoals gezegd, diensten moeten ook de gelegenheid krijgen om, gericht via het hacken van onverdachte derden, dichter bij 'targets' te komen (omschreven als 'operationele kansen tot het benutten van zwakheden bij technische randgebruikers'). Dit zonder die onschuldige 'randgebruikers' daarover in te lichten.

In het algemeen zal een hackbevoegdheid een prikkel zijn voor diensten om kwetsbaarheden te zoeken en zo mogelijk gebruik te maken van zogenaamde zero day vulnerabilities. Dit is echter zeer ongewenst volgens ISOC Nederland: dergelijke zwakheden kunnen door een ieder uitgebuit worden, ook door de targets, terroristen en buitenlandse mogendheden waar de diensten juist tegen in het geweer (willen) komen. Indien dergelijke kwetsbaarheden niet bekend gemaakt worden en niet direct worden gerepareerd, dan is dat schadelijk en gevaarlijk voor iedereen. 'The vulnerabilities they discover affect the security of us all', zoals security expert Bruce Schreier aangeeft.[21] Daarnaast is er een paradox: enerzijds moet een overheid-gerelateerde dienst kunnen hacken, en deze heeft er dus belang bij dat kwetsbaarheden (blijven) bestaan. Terwijl gelijktijdig bedrijven wettelijk verplicht zijn alle mogelijke maatregelen te treffen om hun netwerken te beveiligen inclusief een meldingsplicht wanneer het toch mis gaat. Hoe daarmee om te gaan? Dit is niet de betrouwbare en transparante overheid die we zouden willen zien, vindt ISOC Nederland.

4. Bewaartermijnen

Bewaartermijnen in het wetsvoorstel worden niet gemotiveerd en zijn daarom buitenproportioneel. In artikel 33 staat dat in bulk onderschepte en nog niet 'verwerkte' data drie jaar mogen worden opgeslagen. Als ze na die periode niet relevant blijken te zijn dan 'worden ze terstond vernietigd'. Hetgeen suggereert dat 'relevante data' wel langer dan 3 jaar bewaard worden. Een uiterste periode wordt niet vermeld. En in artikel 30 lid 9 (hackbevoegdheid) staat: gegevens 'worden zo spoedig mogelijk op hun relevantie voor het onderzoek waarvoor ze zijn verworven onderzocht. Gegevens, waarvan is vastgesteld dat deze niet relevant zijn voor het onderzoek dan wel niet op hun relevantie voor het onderzoek zijn onderzocht, worden na een periode van ten hoogste twaalf maanden vernietigd.' Waarom niet-relevante gegevens een jaar bewaren? En gegevens moeten direct worden onderzocht, maar als dat niet gebeurt (?) dan kunnen ze alsnog 12 maanden worden bewaard?

---

inbreuk op het in artikel 8 EVRM neergelegde recht een legitiem doel moet dienen, bij wet moet zijn voorzien en noodzakelijk moet zijn in een democratische samenleving.' Artikel 8 EVRM verwijst niet expliciet naar een vereiste voorafgaande toestemming van een onafhankelijke rechter, maar wat ISOC NL betreft is dat wel de lijn die het Kabinet dient te kiezen wanneer 'alle inhoud', 'ongeacht het communicatiemiddel', 'aan dezelfde eisen' onderworpen wordt.

[21] https://www.schneier.com/blog/archives/2014/05/disclosing_vs_h.html

5. Doelgerichtheid interceptie in bulk en onderverdeling in fasen

De ongerichte en technologie-neutrale ('bulk') interceptiebevoegdheid uit artikel 33 lid 1 kan alleen met voorafgaande toestemming van de Minister worden ingezet. Zie de opmerking hierboven over een voorkeur van ISOC voor een onafhankelijke toetsing vooraf, bij uitstek relevant voor wat betreft deze ultieme bevoegdheid. Daarnaast, als het gaat om de zogenaamde vereiste 'doelgerichtheid' van de inzet van deze bevoegdheid: 'Zo zal in het verzoek onder meer het onderzoek waarvoor de bevoegdheid moet worden ingezet dienen te worden omschreven alsmede het doel wat met de bevoegdheidsuitoefening wordt beoogd. Daarbij kan niet worden volstaan met een globale aanduiding, maar moet dit zo concreet als mogelijk is, dienen te worden ingevuld.' Aldus de MvT op pagina 67. Dat is voor ISOC Nederland een te vage en ruim gedefinieerde en 'ongerichte' doelopvatting. Het is volstrekt onduidelijk aan welke vereisten de formulering van 'onderzoek' en 'doel' moet voldoen, op basis waarvan toestemming verleend wordt.

Artikel 34 richt zich op fase 2, de zogenaamde 'voorverwerking'. Dat suggereert dat die voorverwerking betrekking heeft op de in fase 1 geïntercepteerde data. Dat is ook het geval, echter daarnaast hebben de diensten uit hoofde van artikel 34 ook een bevoegdheid met betrekking tot 'beoogde activiteiten (...) in het cyberdomein waar het gaat om netwerkmonitoring of netwerkdetectie'. De Mvt zegt op blz 71 dat dan 'bijvoorbeeld door de inzet van Deep Packet Inspection-apparatuur, *realtime* en *online* het dataverkeer (wordt) geanalyseerd.' Het is voor ISOC Nederland niet duidelijk hoe deze bevoegdheid zich verhoudt tot de gedefinieerde fasen en de daarbij behorende toestemmingsvereisten. Als zodanig lijkt deze 'cyber' bevoegdheid zelfs verborgen. Is dat de intentie van de wetgever?

6. Verruiming van medewerkingsplicht voor bedrijven: introductie 'aanbieder van communicatiedienst'

In de Telecommunicatiewet (Tw) is bepaald dat de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten verplicht zijn medewerking te verlenen aan de uitvoering van een toestemming tot het aftappen of opnemen van telecommunicatie die over hun telecommunicatienetwerken wordt afgewikkeld dan wel via hen verzorgde telecommunicatie. In artikel 32, zevende lid, wordt voor wat betreft de Wiv de medewerkingsplicht uitgebreid tot de 'aanbieders van een communicatiedienst' op wie niet reeds een medewerkingsverplichting ex artikel 13.2 Tw rust. Op basis van artikel 31 kan men niet anders dan vaststellen dat het de intentie van de wetgever is om *iedere* 'aanbieder', natuurlijk- of rechtspersoon, onder de reikwijdte van de wet te laten vallen: het gaat om een ieder 'die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of die gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst'. Of het nu een zorgaanbieder is of een online-winkel, een onderwijsinstelling of sportclub. Deze categorie aanbieders is in principe grenzeloos, iedere organisatie communiceert met de buitenwereld via een website, en daarom is deze categorie veel te ruim.

7. 'Kostendragerschap'

De kostenregeling voor 'openbare' aanbieders die vallen onder de Telecommunicatiewet, wordt voor die nieuwe uitgebreide categorie 'aanbieders van een communicatiedienst' overgenomen. Zoals de MvT zegt op blz. 61: 'Kort gezegd komt die regeling erop neer dat deze aanbieders de investerings-, exploitatie- en onderhoudskosten die zij moeten maken om (technisch) aftapbaar te zijn, zelf dienen te dragen'. Een eenzijdige last voor deze zeer brede groep van natuurlijke- en rechtspersonen dus. ISOC Nederland daarentegen zou het een goede zaak vinden als de overheid zelf deze (voor een aanbieder aanzienlijke) kosten op zich neemt. Het zou namelijk indirect als een proportionaliteitstoets fungeren: staan de te maken kosten van interceptie echt in verhouding tot de beoogde baten? Wanneer deze kosten eenzijdig bij de aanbieders worden neergelegd dan is van een dergelijke afweging geen sprake.

Daarnaast is het zeer zorgelijk dat de wetgever geen besef heeft van de mogelijke financiële impact voor genoemde aanbieders, zie de Mvt op bladzijden 201 en 202:

'Een gedetailleerd inzicht in de kosten van interceptie van telecommunicatie op kabelgebonden netwerken als hier bedoeld is op dit ogenblik echter nog niet mogelijk. Deze kosten zullen de komende periode in nauw overleg met relevante aanbieders in de telecomsector in kaart worden gebracht. Het overleg met relevante aanbieders in de telecomsector is tevens vereist om te achterhalen hoe deze bevoegdheid in een technisch complexe omgeving op de meest doeltreffende en doelmatige manier kan worden toegepast, met zo min mogelijk inbreuken op de persoonlijke levenssfeer van burgers. Bij de implementatie van de interceptie van telecommunicatie op kabelgebonden netwerken in het kader van de nieuwe wet is voorts sprake van schaalbaarheid in omvang en tijd. De keuzes die hierbij worden gemaakt hebben vanzelfsprekend gevolgen voor het financiële beslag. Mede om ervaring op te doen op grond waarvan gerichte vervolgstappen kunnen worden genomen, zal de interceptie na inwerkingtreding van de wet in de aanvangsjaren tot enkele fysieke toegangspunten beperkt blijven.'

Het lijkt ISOC Nederland erg onwaarschijnlijk dat er bereidwilligheid zal bestaan bij 'relevante aanbieders' om hierover in 'nauw overleg' met de diensten te treden.

Veel erger is dat het hierbovenstaande suggereert dat de diensten 'tevens' niet weten hoe die kabelgebonden interceptie in te richten. En dat de aanbieders daarom moeten bijdragen aan ontwerp en inrichting 'om te achterhalen hoe deze bevoegdheid in een technisch complexe omgeving op de meest doeltreffende en doelmatige manier kan worden toegepast'. Hetgeen de diensten de gelegenheid moet geven om in de 'aanvangsjaren' wat te testen op 'enkele' onduidelijke 'fysieke toegangspunten', 'om ervaring op te doen', waarna de 'beperking' opgeheven kan worden en de inzet van de bevoegdheid uitgebreid kan worden. Dit kan toch niet waar zijn...

8. Delen gegevens met buitenlandse diensten

Artikel 49 beschrijft het delen van onderschepte gegevens met buitenlandse

diensten, enkel met toestemming van de Minister. Zie de eerder aangegeven gewenste onafhankelijke toetsing. 'Bulk' data kunnen worden gedeeld met andere diensten zonder dat deze geëvalueerd zijn door de Nederlandse diensten. Dus wat men deelt is dan niet bekend. ISOC Nederland beseft dat er uitwisseling tussen diensten moet (kunnen) plaatsvinden, indien noodzakelijk. Maar dan wel gericht, met kennis van de inhoud.

Artikel 76 lid 3 zegt dat alvorens tot 'samenwerking' wordt overgegaan met ene buitenlandse dienst, er eerst een 'weging' plaats vindt op basis van een aantal 'criteria': wat is de 'democratische inbedding' van betreffende buitenlandse dienst, hoe zit het met de 'eerbiediging van de mensenrechten' in het land, en hoe zit het met de 'professionaliteit en betrouwbaarheid' van die dienst. Niet alleen worden de termen als 'democratische inbedding', 'professionaliteit' en 'betrouwbaarheid' niet ingevuld, ook niet in de MvT, ernstiger is dat de doorslag om tot samenwerking over te gaan niet expliciet afhankelijk is van deze criteria. Indien noodzakelijk dan vindt 'samenwerking' gewoon plaats. Immers, zie MvT op blz 137, het Kabinet heeft 'aangegeven dat wereldwijde internationale samenwerking voor de inlichtingen- en veiligheidsdiensten een *conditio sine qua non* is'. Het is dus slechts een intentieverklaring, en kan daarom als artikel ook weg gelaten worden want een wassen neus volgens ISOC Nederland.

Practice what you preach: bescherm de publieke kern van het internet

Nogmaals, wat ISOC Nederland betreft is het uitgangspunt van het voorstel, dat wil zeggen de nut en noodzaak er van, niet onderbouwd en is het dus niet aan de orde om over gedetailleerde invulling te spreken. Een volledige heroverweging van de voornemens verdient de voorkeur. ISOC Nederland wijst de Nederlandse regering in dat kader graag op het uit onverdacht neutrale hoek komende rapport 'De publieke kern van het internet' van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR).[22] Volgens de WRR is er een kern van centrale protocollen en technologie van het internet aan te wijzen die als een *mondiaal publiek goed* kan worden aangemerkt. Het internet als publiek goed functioneert alleen als het de kernwaarden universaliteit, interoperabiliteit en toegankelijkheid garandeert en als het de kerndoelen van informatieveiligheid, te weten vertrouwelijkheid, integriteit en beschikbaarheid ondersteunt. Nederland zou als onderdeel van haar diplomatieke agenda de vereiste neutraliteit van die kerninfrastructuur van het internet moeten opnemen:

'Het beschermen van de publieke kern van het internet is bovendien voor Nederland een verlengd nationaal belang. Een dergelijk belang ligt op een lijn met strategische mondiale vraagstukken die als internationaal publiek goed gedefinieerd kunnen worden, zoals het mitigeren van klimaatverandering of de stabiliteit van het financiële systeem. *Voor Nederland is het betrouwbaar functioneren van het internet van vitaal belang voor zijn economie, economische groei en het functioneren van de (digitale) samenleving*. Nederland scoort zeer hoog op internationale ranglijsten over internettoegang en breedbandverbindingen en bevindt zich in de top van OECD-landen met het hoogste percentage van de bevolking dat online aankopen doet. Nederland heeft een levendige internetindustrie en de AMS-IX is een van de grootste Internet

[22] http://www.wrr.nl/publicaties/publicatie/article/de-publieke-kern-van-het-internet-1/

Exchange Points ter wereld. (...) Nederland heeft niet alleen veel mee in termen van een levendige internetindustrie en -cultuur en politiek leiderschap op een aantal dossiers als netneutraliteit, maar kent ook een traditie van idealisme en pragmatisme. Deze traditie zorgde in eerdere tijden voor een relatief vrije informatiecultuur en bloeiende economie in Nederland. Dat kleine staten aan de wieg van internationale normen of diplomatieke doorbraken staan, is bovendien geen uitzondering. *Voor Nederland is het uitwerken en uitdragen van een nieuwe agenda voor internetdiplomatie, met als uitgangspunt het waarborgen van de kern van het internet als een mondiaal publiek goed, een passende nieuwe ambitie. Dat het waarborgen van de publieke kern van het internet ook voor andere staten een verlengd nationaal belang is, kan als frame voor de internationale agenda dienen.'*[23]

Nederland moet niet willen deelnemen aan de wedloop tussen verschillende staten en hun veiligheidsdiensten: de onthullingen van Snowden hebben de schade van de inzet van ongerichte en massale interceptiebevoegdheden door diensten wel voldoende aangetoond, in combinatie met een daarmee samenhangend gebrek aan transparantie en onafhankelijk toezicht. Bovendien is 'het risico levensgroot dat het cumulatieve effect van nationale maatregelen – waarbij staten in toenemende mate tegen elkaar opbieden – resulteert in grote kwetsbaarheden van de kern van het internet als een publieke infrastructuur. In aanvulling hierop *ontstaat op nationaal niveau de paradox dat sommige delen van de overheid dagelijks proberen een betrouwbaar en veilig internet te waarborgen terwijl andere delen van de overheid op dit gebied de risico's juist vergroten.'*[24]

(cursivering door ISOC Nederland)

De WRR stelt in dat kader terecht dat 'Nederland zich met de oprichting van *Freedom Online Coalition* opgeworpen (heeft) als een voorloper op het gebied van de digitale mensenrechten. Nederland zou ook het voortouw kunnen nemen bij een diplomatieke inspanning die het waarborgen van de publieke kern van het internet als centrale inzet heeft.'[25]

ISOC Nederland is het geheel met de WRR eens dat het van zeer groot belang is het functioneren en de integriteit van die publieke kern van het internet, de protocollen en infrastructuur, veilig te stellen en te beschermen tegen oneigenlijke interventies door staten en andere partijen. Waarbij Nederland dan inderdaad goed gepositioneerd is een internationale rol als gidsland op zich te nemen, mits 'we practice what we preach'. Dat laatste is echter niet wat het Kabinet met het wetsvoorstel voor ogen lijkt te hebben...

Namens het bestuur van ISOC Nederland,

Bastiaan Goslings

---

[23] WRR (2015), *De publieke kern van het internet*, Amsterdam University Press, blz 100
[24] Idem, blz 103
[25] Idem, blz 110