Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

Q&A BIJ ZIENSWIJZE CTIVD

T.b.v. technische briefing Tweede Kamer 13 december 2016 over wetsvoorstel Wiv 20..

Algemeen

1. Wat wil de CTIVD bereiken met haar zienswijze?

Het is noodzakelijk dat er een kwalitatief goede wet komt die nu én in de toekomst een duidelijk kader biedt waarbinnen de diensten hun werk effectief uit kunnen voeren. Evenwicht tussen bevoegdheden en waarborgen is daarin essentieel. Dit evenwicht ontbreekt omdat de bevoegdheden uitgebreid en gemoderniseerd zijn, maar de waarborgen daarbij achterblijven.

2. Kan het wetsvoorstel worden verbeterd?

Het wetsvoorstel voorziet in bevoegdheden van de 21ste eeuw maar geeft waarborgen die uit de 20ste eeuw afkomstig zijn.
Het wetsvoorstel is omvangrijk en complex. Het geeft op veel punten een helder kader, m.n. voor de gerichte bevoegdheden die de diensten kunnen inzetten. Verbetering is noodzakelijk waar het gaat om bevoegdheden die niet gericht zijn en waarbij grote hoeveelheden gegevens worden verwerkt. Daar zijn aanvullende waarborgen essentieel. Die waarborgen moeten in de wet verankerd worden.

3. Hoe komen we tot een goed evenwicht?

Bevoegdheden moeten de diensten in staat stellen tijdig dreigingen te onderkennen. Waarborgen moeten bescherming bieden tegen ongeoorloofde inbreuken op onze grondrechten. Zij moeten logischerwijs vooral aanwezig zijn daar waar de inbreuk op grondrechten het sterkst aan de orde is: bij de analyse en het gebruik van gegevens. Als aan elk van deze facetten in de nieuwe wet invulling wordt gegeven, is het evenwicht bereikt.

4. Wat is het beeld dat de CTIVD heeft van huidige bevoegdheden?

Door veranderingen in communicatiemiddelen en mogelijkheden en de alsmaar digitaliserende samenleving is het voor de diensten niet goed mogelijk met de huidige bevoegdheden dreigingen tijdig te kunnen onderkennen. In toenemende mate is sprake van blinde vlekken bij de diensten. Zo is het tegengaan van digitale spionage niet goed mogelijk zonder kabelbulkinterceptie. Op meerdere onderzoeksterreinen is sprake van verminderde opbrengst van bestaande bevoegdheden doordat communicatietoepassingen en infrastructuur voor communicatie zijn veranderd. Bestaande bevoegdheden voldoen niet langer.

5. Hoe verhoudt kabelinterceptie zich met de bescherming van grondrechten en met name persoonsgegevens?

De CTIVD ziet het als haar taak voortdurend te zoeken naar een goede verhouding tussen nationale veiligheid en privacybescherming. De uitbreiding van de interceptiebevoegdheden is noodzakelijk, maar moet wel gepaard gaan met waarborgen die ervoor zorgen dat alleen die gegevens worden verwerkt die absoluut noodzakelijk zijn voor taakuitvoering van de diensten. Als daar invulling aan wordt gegeven en als dat verankerd wordt in de wet, is sprake van een verantwoorde inrichting van de interceptiebevoegdheid.

Autorisatie

6. Voldoet het voorgestelde systeem van autorisatie, toezicht en klachtbehandeling?

Het voorgestelde systeem voldoet formeel aan de normen van het EHRM. Belangrijk is dat er rechtseenheid komt. Het is natuurlijk niet de bedoeling dat de CTIVD elke toets van de TIB achteraf opnieuw gaat doen. In het kader van een operatie in zijn geheel, of de samenwerkingsrelatie met een buitenlandse dienst, kunnen afwegingen over de inzet van een enkele bevoegdheid in een ander licht komen te staan. Er zal aandacht moeten zijn voor de raakvlakken ter voorkoming van een toezichtshiaat.

Toezicht

7. Hoe verhoudt zich autorisatie ten opzichte van toezicht?

De TIB is geen toezichthouder maar een autorisatiecommissie. Autorisatie en toezicht moeten van elkaar onderscheiden worden. De TIB moet de inzet van bevoegdheden vooraf autoriseren. Dat moet binnen een korte tijd en voor alle aanvragen plaatsvinden.

Toezicht ziet op de rechtmatigheid van de uitvoering van de operaties. Dit toezicht kan een operatie of een samenwerkingsrelatie in zijn geheel beoordelen met achterliggende documenten en de rechtmatigheid van de feitelijke inzet van bevoegdheden toetsen.

8. Waarom is het toezicht volgens u in de toekomst niet voldoende effectief?

Het toezicht is niet effectief omdat het ontbreekt aan handvatten voor toezicht op geautomatiseerde gegevensverwerking. In de Memorie van Toelichting wordt steeds benadrukt dat de CTIVD overal bij kan en alles kan zien. Dat is zo en dat is ook uitermate belangrijk. Maar zonder toetsbare normen en instrumenten waarmee de kwaliteit van geautomatiseerde gegevensverwerking wordt geborgd, kan het toezicht zich niet goed richten en is effectief toezicht niet mogelijk.

9. Wat is toezicht op geautomatiseerde gegevensverwerking?

Toezicht op geautomatiseerde gegevensverwerking houdt in dat de CTIVD kan toetsen of de diensten voldoen aan hun plicht ervoor te zorgen dat automatische processen van gegevensverwerking voldoen aan juridische standaarden en technische kwaliteitsstandaarden.

Voorbeelden van zulke processen zijn:
- een applicatie waarmee grote gegevensbestanden worden doorzocht;
- een systeem dat gegevens beschikbaar maakt voor bepaalde medewerkers en anderen daartoe uitsluit;
- het automatisch filteren van gegevens om deze vervolgens op te slaan of te vernietigen;
- de automatische vernietiging van gegevens als de bewaartermijn afloopt;
- een applicatie waarmee gegevens met andere gegevens worden vergeleken;
- het automatisch binnenhalen van gegevens als daarvoor toestemming is verleend.

Doordat de diensten meer en meer te maken hebben met grote hoeveelheden gegevens, wordt ook steeds meer gewerkt met geautomatiseerde processen voor de verwerking van die gegevens. Het is belangrijk dat daarvoor een zorgplicht geldt. Dit betekent dat de diensten zelf verantwoordelijkheid moeten nemen voor de kwaliteit en rechtmatigheid van de inrichting en werking van deze processen en dit ook zelf periodiek moeten controleren. De CTIVD moet daar vervolgens toezicht op houden.

10. Moet de wet worden aangepast voor effectief toezicht?

De CTIVD heeft toegang tot alle gegevens bij de diensten. Om te waarborgen dat de geautomatiseerde verwerking van grote hoeveelheden gegevens rechtmatig en kwalitatief goed gebeurt, is meer nodig dan toegang tot gegevens alleen. Het is daarvoor van belang dat de diensten een goed beleid voeren, dat de inrichting van processen zelf aan standaarden voor kwaliteit en rechtmatigheid voldoen, dat de privacybescherming daarin wordt betrokken en dat geregeld wordt gecontroleerd wat de werking is van deze processen m.b.t. de analyse en het gebruik van gegevens. Dit is een verantwoordelijkheid die vanzelfsprekend bij de diensten ligt. De CTIVD kan vervolgens, doordat zij toegang heeft tot alle gegevens, erop toezien dat die verantwoordelijkheid goed wordt ingevuld. Zonder toetsbare normen en instrumenten waarmee de kwaliteit van verwerkingsprocessen wordt geborgd, is goed toezicht hierop niet mogelijk. Als het gaat om het automatisch verwerken van grote hoeveelheden gegevens, is er meer nodig dan het enkele feit dat de toezichthouder gegevens kan bekijken.

11. Het wordt technischer en complexer, kan de toezichthouder het wel bijbenen?

Naast juridische en operationele deskundigheid, heeft de CTIVD ook technische expertise aangetrokken en wil zij dit in de toekomst verder uitbouwen. De CTIVD is momenteel bezig met het inrichten van een ICT unit die zich bezighoudt met het ontwikkelen van systeemtoezicht.

Systeemtoezicht richt zich niet op de vraag of wettelijke regels zijn nageleefd (=klassiek toezicht), maar richt zich op de wijze waarop de naleving van wettelijke regels is geborgd. Het gaat bijvoorbeeld om de mate waarin medewerkers interne regels kennen, of er procedures en/of afspraken zijn die de naleving van wetten en regels garandeert, of er controlemechanisme zijn binnen de diensten en of de technische systemen zo zijn ingericht dat daarmee invulling wordt gegeven aan wettelijke waarborgen. In het geval van de CTIVD zal het toezicht altijd een combinatie van klassiek en systeemtoezicht zijn.

Interceptie

12. Wat is eigenlijk onvoldoende geregeld in het wetsontwerp?

Het opslaan, analyseren en gebruiken van grote hoeveelheden gegevens is onvoldoende ingeperkt in het wetsvoorstel. Er moet meer duidelijkheid komen wanneer welke gegevens vernietigd moeten worden.

Met de bevoegdheid om de kabel in bulk te intercepteren is het mogelijk grote hoeveelheden gegevens te verzamelen. Het gaat daarbij ook om communicatie van heel veel personen die geen onderzoek door de diensten rechtvaardigen. Voor de bescherming van grondrechten is het essentieel dat gegevens zo gericht mogelijk worden verzameld en dat die gegevens zo snel mogelijk worden beperkt tot die gegevens die echt nodig zijn voor de bescherming van de nationale veiligheid. Hiervoor geeft de wet te weinig waarborgen.

13. Waarom moet er aanvullende waarborgen komen?

De uitbreiding van de interceptiebevoegdheden is noodzakelijk, maar moet wel samen gaan met voldoende waarborgen. Waarborgen moeten ervoor zorgen dat alleen die gegevens worden verwerkt die absoluut noodzakelijk zijn voor taakuitvoering van de diensten.

14. Welke waarborgen zijn essentieel?

De waarborgen die zorgen voor verantwoorde databeperking zijn essentieel.

Het gaat allereerst om het algemene vereiste dat de inzet van bevoegdheden zo gericht mogelijk moet zijn. Dit vereiste zorgt ervoor dat bulkinterceptie alleen wordt ingezet indien er geen valide gerichte alternatieven zijn. Dit is een andere toets dan de subsidiariteitstoets, omdat die toets wettelijk gezien alleen uitkomt bij het middel dat het minste nadeel oplevert voor de betrokken persoon of organisatie. Verder gaat het om wettelijke plichten die ervoor zorgen dat de opslag, analyse en het gebruik van de gegevens die zijn verzameld zo doelgericht mogelijk plaatsvinden. Steeds moet worden beoordeeld of gegevens vernietig kunnen worden.

1. Zo moet in de wet worden verankerd dat alleen gegevens mogen worden opgeslagen die gerelateerd zijn aan een onderzoeksopdracht.
2. Wanneer vervolgens op basis van bijvoorbeeld search wordt vastgesteld dat een gegeven toch niet gerelateerd is aan een onderzoeksopdracht, moet het gegeven vernietigd worden. De plicht hiertoe moet in de wet komen te staan (doorlopende vernietigingsplicht).
3. Gegevens die gerelateerd zijn aan een onderzoeksopdracht mogen worden bewaard tot de bewaartermijn afloopt. Daarbij moet onderscheid worden gemaakt in de bewaartermijn voor inhoud en de bewaartermijn voor metadata, waarbij de laatste gekoppeld moet worden aan meer waarborgen voor metadata-analyse.
4. Totdat de bewaartermijn is verlopen hebben de diensten de tijd selectie toe te passen. Deze bevoegdheid moet doelgerichter worden gemaakt door een extra drempel voor selectie in de wet op te nemen.
5. Nadat gegevens zijn geselecteerd moeten ze worden beoordeeld op relevantie. Niet relevante gegevens moeten worden vernietigd. Hiervoor moet een plicht in de wet opgenomen worden.

Dus:
- Wettelijke plicht om de opslag van gegevens te beperken (alleen wat gerelateerd is aan een onderzoeksopdracht);
- Wettelijke verankering van de doorlopende vernietigingsplicht;
- Onderscheid tussen metadata en inhoud in bewaartermijnen gekoppeld aan meer waarborgen voor metadata-analyse;
- Extra drempel voor selectie;
- Wettelijke verankering van de plicht geselecteerde gegevens te beoordelen op relevantie.

15. Hoe verhoudt zich het vereiste "zo gericht mogelijk" ten opzichte van proportionaliteit/ subsidiariteit?

Het vereiste dat de inzet van bevoegdheden zo gericht mogelijk moet zijn, zorgt ervoor dat de diensten bij de keuze voor bulkinterceptie moeten meewegen of er ook gerichte alternatieven zijn. Met bulkinterceptie wordt inbreuk gemaakt op de grondrechten van veel personen die geen onderzoek door de diensten rechtvaardigen. Het is daarom belangrijk dat hier terughoudend mee wordt omgegaan, zeker met gerichte bevoegdheden hetzelfde doel kan worden bereikt.

De vereisten van proportionaliteit en subsidiariteit ondervangen dit niet per se. De afwegingen die hierbij plaats moeten vinden, richten zich wettelijk gezien alleen op nadelen voor de betrokken persoon of organisatie. De inbreuk die op de grondrechten van talloze anderen wordt gemaakt, hoeft niet in de weging van proportionaliteit en subsidiariteit te worden meegenomen. En zo kan het zijn dat de inzet van bulkinterceptie en selectie minder inbreukmakend is voor de betrokken persoon dan de inzet van een gerichte telefoontap, bijvoorbeeld doordat niet alle communicatie van een bepaalde telefoon wordt binnengehaald. Terwijl we het er allemaal over eens zijn dat een gerichte telefoontap in veel gevallen toch de voorkeur moet hebben, omdat daarbij uitsluitend op de grondrechten van het doelwit inbreuk wordt gemaakt.

16. Wat is verantwoorde databeperking?

Met de bevoegdheid om de kabel in bulk te intercepteren is het mogelijk zeer grote hoeveelheden gegevens te verzamelen. Het gaat daarbij ook om communicatie van heel veel personen die geen onderzoek door de diensten rechtvaardigen. Voor de bescherming van grondrechten is het essentieel dat gegevens zo gericht mogelijk worden verzameld en dat die gegevens zo snel mogelijk worden beperkt tot die gegevens die echt nodig zijn voor de bescherming van de nationale veiligheid. Hiervoor geeft de wet te weinig waarborgen.

17. Waarom een plicht opslag van gegevens te beperken?

De bevoegdheid van bulkinterceptie is in het wetsvoorstel onderzoeksopdrachtgerichte interceptie genoemd. Het is niet langer 'ongericht' zoals in de Wiv 2002, maar 'onderzoeksopdrachtgericht'. Dit impliceert dat bij de interceptie alleen gegevens worden binnengehaald die gerelateerd zijn aan een onderzoeksopdracht. Feit is dat bij de interceptie zelf ook gegevens worden binnengehaald die geen enkele relatie hebben met een onderzoeksopdracht. De 'onderzoeksopdrachtgerichtheid' wordt in belangrijke mate bepaald door de keuze om bepaalde gegevens wel op te slaan en andere gegevens te vernietigen. Daar zijn extra handelingen voor nodig. Die extra handelingen bestaan in de praktijk uit het filteren van de gegevens. Dat dit plaatsvindt, is niet geborgd. Het is essentieel dat de opslag van gegevens wordt beperkt tot de onderzoeksopdrachten en dat dit in de wet wordt geregeld.

18. Waarom een onderscheid tussen metadata en inhoud?

Er bestaat verschil in de noodzaak van het bewaren van metadata en van inhoud. De in de Memorie van Toelichting aangedragen argumenten en voorbeelden gaan over metadata, niet zozeer over inhoud. Het is dus logisch een onderscheid te maken. Het is niet noodzakelijk inhoud net zolang te bewaren als metadata.
Of vervolgens een bewaartermijn van 1 of 3 jaar zou moeten gelden is arbitrair. De lengte van de bewaartermijn voor metadata zou in ieder geval afhankelijk moeten zijn van de waarborgen die zijn ingericht voor metadata-analyse. Dat is immers waar de inbreuk vooral plaatsvindt. De regeling voor metadata-analyse moet op twee punten een versterking van waarborgen krijgen: t.a.v. de reikwijdte van de bijzondere bevoegdheid en de daarbij geldende toestemmingstermijn.

19. Is het verzamelen van metadata niet zo inbreukmakend?

De opslag en analyse van metadata kan onder omstandigheden net zo inbreukmakend zijn als de opslag en analyse van inhoud van communicatie. Daarbij moet wel de nadruk worden gelegd op de analyse. Daar vindt de sterkste inbreuk plaats dus daar moeten vooral waarborgen worden ingesteld. Het verschil in bewaartermijn wordt niet zozeer ingegeven door het inbreukmakende karakter van het één boven het ander, maar door het verschil in de noodzaak van het bewaren.

20. Wat wordt bedoeld met de extra voorwaarde voor selectie?

De CTIVD adviseert search als voorwaarde voor selectie te stellen, als een selectiecriterium niet direct gekoppeld kan worden aan een persoon of organisatie waarvoor de minister toestemming heeft verleend. De relevantie van het selectiecriterium moet dan eerst worden getoetst met behulp van search.
De minister geeft toestemming voor de inzet van selectie t.a.v. bepaalde personen of organisaties. De concrete invulling van de selectie vindt plaats door het toepassen van bepaalde selectiecriteria, zoals nummers en trefwoorden. Goede selectiecriteria kunnen worden toegespitst op een persoon of organisatie waarvoor de minister toestemming heeft gegeven. Deze selectiecriteria kunnen relevante gegevens opleveren over de desbetreffende persoon of organisatie (bijvoorbeeld een telefoonnummer van iemand waarvan bekend is dat hij is uitgereisd). In de praktijk bestaat er echter een motiveringsprobleem. Veel selectiecriteria kunnen niet worden gekoppeld aan een persoon of organisatie en kunnen dus niet goed worden gemotiveerd. Het is niet op voorhand duidelijk dat deze selectiecriteria relevante gegevens kunnen opleveren. Het is dan meer een kwestie van uitproberen. Hiervoor moet een waarborg komen. De relevantie van het selectiecriterium moet eerst worden getoetst met behulp van search. Door te searchen kan worden bekeken of met het selectiecriterium daadwerkelijk gegevens kunnen worden geselecteerd die van waarde zijn voor het onderzoek. Is dat het geval dan kan het selectiecriterium gebruikt worden. Search is daarmee een voorwaarde voor selectie. Het zorgt voor goede selectiecriteria. Search als voorwaarde voor selectie is niet in de wet of de toelichting opgenomen.

21. Wat is beoordeling op relevantie? Staat dat niet in de wet?

De wet lijkt er ruimte voor te laten dat geselecteerde gegevens als relevante gegevens (en dus ook als geëvalueerde gegevens) kunnen worden beschouwd zonder dat daar een nadere beoordeling aan te pas komt. Dit zou als resultaat hebben dat alle gegevens die zijn geselecteerd, als geëvalueerd worden beschouwd en zonder meer gebruikt en bewaard mogen worden. Het is essentieel dat eerst nog een beoordeling op relevantie plaatsvindt aan de hand van de inhoud van de communicatie die is geselecteerd. Gegevens die niet relevant zijn moeten worden vernietigd.

Het wetsvoorstel vereist een zelfde beoordeling op relevantie bij gegevens die zijn verzameld door de inzet van andere bijzondere bevoegdheden. Daar geldt een termijn van een jaar om de ongeëvalueerde gegevens te evalueren, d.w.z. te beoordelen op relevantie.

Geautomatiseerde gegevensverwerking

22. Wat is Big Data analyse?

Big Data analyse is het geautomatiseerd analyseren van een grote hoeveelheid gegevens, bijvoorbeeld met behulp van een algoritme (reeks instructies die naar een bepaald doel leidt, het weegt de data ten opzichte van elkaar).

De WRR stelt dat het vaak gaat om:

- Secundair gebruik van gegevens, d.w.z. dat de gegevens oorspronkelijk voor een ander doel zijn verzameld.
- Datagedreven analyse, d.w.z. niet op een persoon of organisatie gericht (zonder concreet aanknopingspunt).

Big Data analyse is onderdeel van wat in het wetsvoorstel 'geautomatiseerde data-analyse' heet.

23. Hoe passen de diensten Big Data analyse toe?

Geautomatiseerde analyseprocessen worden volgens de Memorie van Toelichting sinds jaar en dag toegepast binnen de diensten. Het gaat daarbij voornamelijk om data-analyse die gericht is op personen en organisaties. De diensten passen steeds vaker ook datagedreven, d.w.z. ongerichte vormen van geautomatiseerde data-analyse toe, zoals Big Data analyse.
Geautomatiseerde data-analyse wordt veelvuldig toegepast, ook t.a.v. gegevens die in grote hoeveelheden zijn verzameld (bulkinterceptie).

24. Wanneer geeft de minister/TIB toestemming voor Big Data analyse?

Er is één specifieke vorm van geautomatiseerde data-analyse waarvoor toestemming van de minister en TIB is vereist. Het gaat om bulk metadata-analyse gericht op het identificeren van personen of organisaties.

De CTIVD vindt dat voor alle vormen van geautomatiseerde data-analyse die is gericht op personen of organisaties en die een stelselmatig karakter heeft toestemming van minister en TIB vereist zou moeten zijn. Stelselmatig houdt in dat een min of meer volledig beeld van een bepaald aspect van iemands privéleven wordt verkregen, bijvoorbeeld op welke locaties iemand gedurende een bepaalde tijd is geweest of welke websites iemand heeft bezocht. Dat zou ook als een bijzondere bevoegdheid moeten gelden.

25. Welke waarborgen zijn nodig voor Big Data analyse?

Voor datagedreven (ongerichte) vormen van geautomatiseerde data-analyse, zoals Big Data-analyse, heeft voorafgaande toestemming van de minister weinig waarde. Big Data-analyse is niet gericht op een persoon of organisatie en is dus niet goed vooraf te motiveren. Het is daarom essentieel dat waarborgen worden ingericht voor de kwaliteit van de analyse en het gebruik van de gegevens.
De CTIVD stelt voor een zorgplicht in te stellen, niet alleen voor Big Data analyse maar voor alle vormen van geautomatiseerde gegevensverwerking die bij de diensten plaatsvindt.

26. Is Big Data analyse hetzelfde als het grootschalig aftappen?

Big Data analyse kan toegepast worden op allerlei grote hoeveelheden gegevens en dus ook op gegevens die grootschalig zijn afgetapt (bulkinterceptie). Het is niet hetzelfde en het is ook niet altijd aan elkaar gekoppeld. Big Data analyse wordt niet altijd toegepast op bulkinterceptie. Er zijn andere vormen van data-analyse, die zijn gericht op personen en organisaties, waarmee bulkinterceptie geanalyseerd kan worden. Verder geldt dat Big Data analyse ook op andersoortige data kan worden toegepast, het hoeft niet altijd om bulkinterceptie te gaan.

27. Wat is het risico van geautomatiseerde gegevensverwerking?

Er is sprake van risico's voor de bescherming van grondrechten, omdat geautomatiseerde gegevensverwerking vaak gaat om de verwerking van persoonsgegevens.
Ook zijn er risico's die inherent zijn aan het automatische en complexe karakter van de gegevensverwerking, zoals het niet meer kunnen herleiden waar de gegevens vandaan komen en in welke context ze moeten worden geplaatst, onzekerheid over de betrouwbaarheid van de gegevens, gebrek aan inzicht in de gebruikte analysemethode en ga zo maar door. Dit kan leiden tot foute uitkomsten of uitkomsten waar een bepaalde *bias* in zit, zonder dat dit zichtbaar is.
Daar komt bij dat veel wettelijke waarborgen in de praktijk zullen worden ingevuld door een geautomatiseerd proces, bijvoorbeeld het vernietigen van gegevens nadat de bewaartermijn is afgelopen of het stoppen van het tappen omdat de toestemming van de minister niet meer geldig is. Die geautomatiseerde processen zijn dus erg belangrijk. Dan is het essentieel dat de kwaliteit van die processen geborgd wordt en dat dit gecontroleerd wordt.

28. Waarom een zorgplicht?

Een zorgplicht houdt in dat de diensten zelf de verantwoordelijkheid moeten nemen voor de kwaliteit van de geautomatiseerde gegevensprocessen en daar ook zelf kwaliteitschecks op moeten uitvoeren. Het geeft de diensten de ruimte om de geautomatiseerde processen naar eigen inzicht in te richten en toe te passen. Dat is van belang want het gaat hier om de *core business* van de AIVD en de MIVD.
Die verantwoordelijkheid is onlosmakelijk onderdeel van de verantwoordelijkheid van de diensten is als gewerkt wordt met steeds grotere gegevensbestanden en (geautomatiseerde) analyse van die bestanden De gehele overheid en private sector is gebonden aan bepaalde kwaliteitsstandaarden voor de verwerking van persoonsgegevens op basis van de Algemene Verordening Gegevensbescherming. De AVG en Wet bescherming persoonsgegevens (per mei 2018) zijn niet van toepassing op de geheime diensten. De nieuwe Wiv moet daar dus in voorzien. Het kan niet zo zijn dat juist diensten die voortdurend in het geheim geautomatiseerd persoonsgegevens verwerken niet ten minste aan diezelfde standaarden zijn gebonden.
Verder stelt het de CTIVD in staat erop toe te zien of de diensten hun zorgplicht voldoende naleven en hierover te rapporteren aan het Parlement.

29. Wat houdt de zorgplicht concreet in?

De zorgplicht houdt in dat de diensten in moeten kunnen staan voor de kwaliteit van:
- de gegevensvergaring;
- de gebruikte gegevens;
- de modellen, algoritmes, technieken en methoden die worden toegepast; en
- de resultaten.

Daarvoor moeten enkele instrumenten in de wet worden opgenomen:
1. gegevensbeschermingsbeleid (aandacht voor risico's, goede inrichting systemen)
2. gegevensbeschermingseffectbeoordeling (bij grote projecten van gegevensverwerking een impactanalyse op persoonlijke levenssfeer en verwachte effectiviteit)
3. audits (m.b.t. gebruikte databestanden, analysemethoden en resultaten)

30. Is in het wetsvoorstel een zorgplicht opgenomen?

De zorgplicht die is opgenomen (artikel 24) stelt dat de technische, personele en organisatorische maatregelen die worden genomen in overeenstemming moeten zijn met de wet. Dat is veel beperkter. Dat geeft geen waarborgen dat de processen die worden ingericht moeten voldoen aan juridische en kwaliteitsstandaarden.

Hacken

31. Welke aanvullende waarborgen zijn nodig bij hacken?

- Er moet duidelijkheid zijn over het derden begrip.
- De inzet van hacken via derden mag alleen als dat onvermijdelijk is.
- Gegevens van derden moeten terstond vernietigd worden.
- De beschrijfmogelijkheid moet worden beperkt.

32. Wat kan er allemaal gehackt worden?

Voorbeelden van hacken zijn het binnendringen van een smartphone, emailaccount, laptop of server. In de context van de wet spreken we van het binnentreden van een geautomatiseerd werk. Dat moet dan voldoen aan drie cumulatieve voorwaarden: het moet gegevens kunnen opslaan, verwerken en verzenden.

33. Waarom hacken via derden?

Hacken via derden moet mogelijk zijn als de gegevens niet op andere manier kunnen worden verkregen. In de wet moet worden verankerd dat het hacken via derden alleen is toegestaan als dat onvermijdelijk is om binnen te kunnen dringen in het geautomatiseerd werk van het doelwit. Die waarborg ontbreekt in het wetsvoorstel.
Onvermijdelijk wil zeggen dat er geen andere reële mogelijkheid is, gelet op de specifieke omstandigheden. Dat moet schriftelijk worden gemotiveerd.

34. Wat is "directe relatie"?

Het aantal technische schakels waarbij nog kan worden gesproken van een directe technische relatie hangt af van omstandigheden en zal telkens moeten worden beoordeeld door de minister, TIB en CTIVD.

Samenwerking buitenlandse diensten

35. Wat zijn de samenwerkingscriteria?

In het wetsvoorstel zijn opgenomen:

1. Democratische inbedding
2. Respect voor mensenrechten
3. Professionaliteit en betrouwbaarheid

Daar moeten in ieder geval aan worden toegevoegd:

4. Mate van gegevensbescherming
5. Wettelijke bevoegdheden en technische mogelijkheden van een buitenlandse dienst

36. Welk fundament ontbreekt in de wet voor samenwerking?

De diensten moeten toetsen of met een buitenlandse dienst samengewerkt mag worden en hoe ver de samenwerking kan gaan. Die toets gebeurt op basis van samenwerkingscriteria en moet ook nu al verricht worden. Er ontbreken drie dingen in het wetsvoorstel:

1. Niet alle samenwerkingscriteria staan er in (zie antwoord vorige vraag);
2. De wet bevat een overgangsregeling waardoor deze systematiek 2 jaar buiten toepassing wordt verklaard terwijl de huidige wet sinds 2002 richting geeft op dit punt;
3. Een uitzonderingsregel heeft een algemene werking gekregen. Daardoor is het mogelijk buiten de toets van samenwerkingscriteria om gegevens te verstrekken, zonder dat hier waarborgen tegenover staan.

Dit alles kan eenvoudig herstelt worden door enkele aanpassingen te maken in de wetstekst.

37. De uitzonderingsregel problematisch?

In de memorie van toelichting wordt een uitzonderingsregel in het algemeen van toepassing verklaard. Daardoor is het mogelijk buiten de toets van samenwerkingscriteria om gegevens te verstrekken, zonder dat hier waarborgen tegenover staan. Voor gegevensverstrekking in het kader van de eigen taakuitvoering hoeft geen samenwerkingsrelatie te bestaan. Het gaat hierbij om het merendeel van de gegevensverstrekkingen.
De CTIVD vindt dat voor de uitzondering een betere regeling moet worden getroffen. In het algemeen geldt dat gegevensverstrekking plaatsvindt in het kader van een samenwerkingsrelatie waarbij een toets van de samenwerkingscriteria plaatsvindt. In het uitzonderlijke geval dat de diensten gegevens willen verstrekken zonder dat sprake is van een samenwerkingsrelatie, moet die mogelijk zijn onder de voorwaarden dat:

- sprake is van een dringende en gewichtige reden; en
- de minister toestemming heeft verleend.

38. Worden verschoningsgerechtigden voldoende beschermd?

Het wetsvoorstel biedt alleen een regeling voor advocaten en journalisten. De CTIVD vindt geen verklaring voor een onderscheid tussen rechtens erkende verschoningsgerechtigden. Waarom genieten notarissen, artsen en geestelijken niet eenzelfde bescherming?

Beperking is dat bij een voorafgaande rechterlijke toets geen klachtenbehandeling over die toets zal kunnen plaatsvinden.

Het wetsvoorstel geeft geen regeling voor de situatie dat met het verwerken van gegevens uit een bijzondere bevoegdheid, bijvoorbeeld het uitwerken in een tapverslag, gegevens worden bewerkt die betrekking hebben op de identiteit van een bron van een journalist. Zo'n regeling wordt wel gegeven voor de verwerking van communicatie tussen de advocaat en zijn cliënt.