Privacy

Big data

Een Amerikaanse man krijgt van een warenhuis kortingsbonnen voor zwangerschapsproducten thuisgestuurd. Het bedrijf blijkt eerder op de hoogte van de zwangerschap van zijn tienerdochter dan hij. Het meisje had daar nog helemaal geen zwangerschaps- of babyspullen gekocht. Hoe kan dit? De data-analist van het warenhuis had een lijst opgesteld van 25 producten die een indicatie kunnen zijn voor zwangerschap, zoals voedingssupplementen als zink en foliumzuur. Aan de hand hiervan kon hij inschatten of iemand zwanger was.

Big data: Overheid, instellingen en bedrijven registreren wat mensen doen en slaan dat op. Wat we op internet zoeken, wat we kopen, wie onze vrienden zijn en waar we naar toe gaan. Het gaat om enorme hoeveelheden gegevens over personen en hun gedrag, verzameld door onder andere internetmonitoring en GPS-systemen. Deskundigen analyseren de gegevens en ontwikkelen profielen. Verzekeraars gebruiken profielen voor risicotaxaties, veiligheidsdiensten voor de inschatting of iemand een bedreiging vormt en bedrijven als Facebook voor reclamedoeleinden.

Organisaties wisselen steeds vaker gegevens uit. Dat kunnen overheidsinstellingen onderling zijn, maar ook publieke en private partijen. Denk bijvoorbeeld aan de verstrekking van parkeergegevens aan de Belastingdienst.

Big data risico voor privacy en andere mensenrechten

Big data bieden enorme mogelijkheden. Ze zijn een bron van economische waarde en innovatie. Op basis van big data zijn bijvoorbeeld epidemieën of de koers van een tornado beter voorspelbaar en kunnen bedrijven inspelen op de behoeften van consumenten. De keerzijde is dat er grote privacyrisico's verbonden zijn aan het gebruik van big data. Zelfs geanonimiseerde gegevens zijn soms terug te voeren op individuele personen.

Naast het recht op bescherming van de privacy kunnen ook andere mensenrechten in het gedrang komen door big data. Zo ligt bij het gebruik van risicoprofielen het gevaar van discriminatie op de loer. Dit is bijvoorbeeld het geval als persoonskenmerken als ras of afkomst een rol spelen bij het bepalen of iemand een bedreiging voor de veiligheid vormt. ■

Voorspellingen van gedrag zijn niet altijd onschuldig

In de kern gaat alles bij big data om voorspellingen. Via wiskundige methodes worden uit enorme hoeveelheden gegevens waarschijnlijkheden berekend. Mensen worden benaderd en behandeld op basis van 'verondersteld toekomstig gedrag'. Kohnstamm, voorzitter van het College bescherming persoonsgegevens, spreekt in dit kader over het gevaar van 'digitale predestinatie'. Voorspellingen kunnen gaan over koop- en reisgedrag, maar ook over minder onschuldige zaken zoals uitkeringsfraude, criminaliteit en terrorisme. Er is een risico dat het behoren tot een bepaalde groep een rol speelt om iemand als verdacht te bestempelen. Dit staat op gespannen voet met het recht op bescherming van de privésfeer en het discriminatieverbod. Ook het rechtsbeginsel 'het vermoeden van onschuld' komt hierdoor in het gedrang. ■

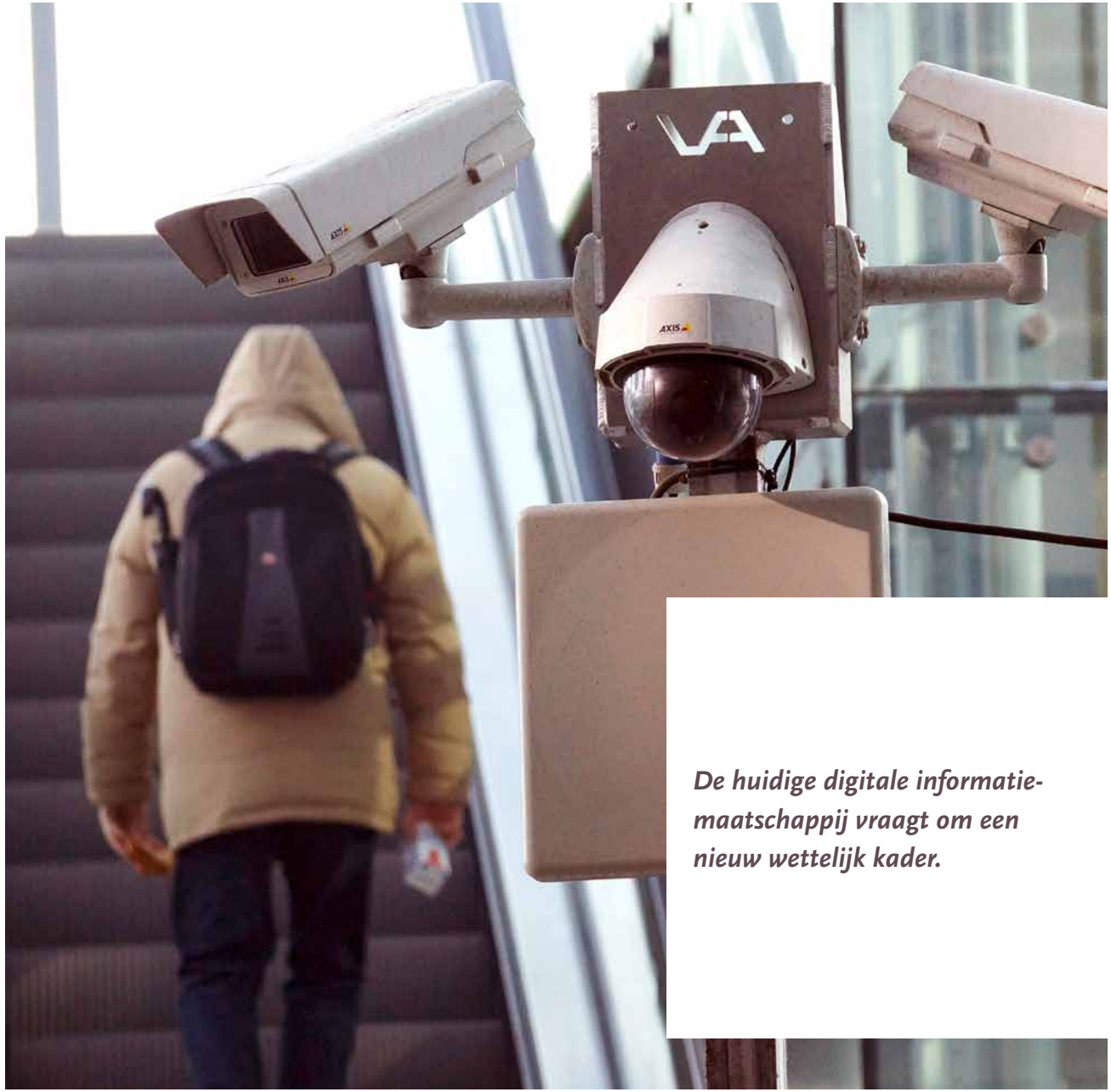
Herbezinning op privacybescherming is nodig

Een fundamentele herbezinning op wettelijke bescherming van de privacy is nodig. De huidige wet beschermt het individu tegen inbreuken op zijn privéleven. De uitgangspunten zijn dat opslag van gegevens alleen gebeurt als het echt nodig is, dat gegevens alleen voor een strikt omschreven doel worden verzameld en opgeslagen, en dat elke burger zelf toestemming geeft voor het verwerken van zijn gegevens.
Bij de verzameling van big data ligt het doel waarvoor gegevens worden verzameld echter van tevoren niet vast en kan in potentie iedereen voortdurend voorwerp zijn van een gerichte of ongerichte inbreuk op zijn persoonsgegevens. Nu of in de toekomst, zonder dat te merken of zonder te weten wat de consequenties zijn. Dat maakt het voor individuele burgers praktisch onmogelijk geïnformeerde toestemming te geven of zich te verzetten.
Er is dus behoefte aan mechanismen die zich niet alleen richten op bescherming van afzonderlijke individuen, maar op bescherming van de massa: het collectief van individuen van wie gegevens verzameld wordt. ■

Verlenen van toestemming is niet langer voldoende waarborg

Door gebruik van een zoekmachine zoals Google, of gebruik van e-mail, Facebook of een app geeft men impliciet toestemming. Dat is geen bewuste keus voor toestemming in opslag, gebruik of doorgeven van gegevens. Is er zelfs wel een keuze voor wie volwaardig wil deelnemen aan het moderne leven? Toestemming wordt dan een wassen neus. Een ander probleem is dat organisaties gegevens voor een ander doel gaan gebruiken dan waarvoor zij in eerste instantie zijn verzameld en waarvoor toestemming is gegeven.

Kortom: de huidige digitale informatiemaatschappij vraagt om een nieuw wettelijk kader, waarin de rechtsbescherming niet louter afhangt van het inroepen daarvan door het individu zelf. Of van een onafhankelijke toezichthouder, die met een beperkte hoeveelheid middelen nooit alles kan onderzoeken. Nieuwe (Europese) wetgeving zal dataverzamelaars moeten verplichten in hun systemen waarborgen en controlevormen in te bouwen om het gevaar van discriminerende predestinatie en stereotypering te voorkomen en te bestrijden. ■



De huidige digitale informatie-maatschappij vraagt om een nieuw wettelijk kader.

Bewaarplicht telecommunicatiegegevens behoeft wijziging

In november 2014 publiceerde de minister van Veiligheid en Justitie een conceptwetsvoorstel dat een aanpassing van de bestaande bewaarplicht voor telecommunicatiegegevens van zowel telefoon- als internetverkeer moet gaan regelen. Aanleiding voor dit wijzigingsvoorstel van de Telecommunicatiewet en het Wetboek van Strafvordering is een uitspraak van het Europees Hof van Justitie van 8 april 2014. Het Hof bepaalde daarin dat een algemene bewaarplicht van zogeheten verkeersgegevens in strijd is met het fundamentele recht op de bescherming van persoonsgegevens zoals dat is verankerd in Europees recht. Diverse organisaties spanden vervolgens een procedure aan bij de rechtbank Den Haag. Bij vonnis in kort geding stelde de rechtbank op 11 maart 2015 de Wet bewaarplicht telecommunicatiegegevens buiten werking. ■

Noodzaak bewaarplicht niet aangetoond

Het conceptwetsvoorstel past de bestaande bewaarplicht op onder meer de volgende punten aan: (1) introductie van een voorafgaande toetsing door een rechter-commissaris op vorderingen van officieren van justitie tot verstrekking van historische telecommunicatiegegevens; (2) introductie van een onderscheid tussen een bewaartermijn van 12 maanden voor telefoniegegevens en de termijn van raadpleging ervan tussen de 6 en 12 maanden, afhankelijk van de aard van het misdrijf.

Deze voorgestelde verbeteringen nemen nog niet alle mensenrechtelijke bezwaren tegen de bewaarplicht weg. De toelichting bij het voorstel en de debatten in het parlement maken niet duidelijk waarom het beslist noodzakelijk is de historische telefoon- en internetgegevens van bijna alle Nederlanders gedurende 6 tot 12 maanden te bewaren. Ondanks dat politie en justitie de afgelopen jaren ruime ervaring met een bewaarplicht hebben kunnen opdoen, zijn geen gegevens overgelegd waaruit de dwingende maatschappelijke noodzaak tot deze ingrijpende maatregel blijkt. Evenmin is er antwoord op de vraag of er geen andere, minder ingrijpende middelen mogelijk zijn om hetzelfde doel te bereiken. ■

Onevenredige inbreuk op de persoonlijke levenssfeer

De bewaarplicht houdt in dat bedrijven die telefonie en internet aanbieden verplicht zijn bepaalde verkeersgegevens te bewaren zodat deze beschikbaar blijven in het geval de gegevens noodzakelijk zijn in een opsporingsonderzoek naar een ernstig strafbaar feit. Omdat het echter om een algemene bewaarplicht gaat, is sprake van een inbreuk op de persoonlijke levenssfeer van iedereen in Nederland. Het Europese Hof van Justitie bepaalde in zijn uitspraak dat bij een bewaarplicht speciale aandacht nodig is voor de positie van personen met een beroepsgeheim, zoals advocaten en artsen.

Het wetsvoorstel doet dat onvoldoende. Het kabinet meent dat er voldoende garanties zijn door de manier waarop opsporingsdiensten toegang tot de bewaarde gegevens krijgen. Dat is echter niet in overeenstemming met het uitgangspunt dat het enkel bewaren van gegevens al een inbreuk op de privacy is. Die inbreuk mag niet onevenredig zijn en dat is door het algemene karakter van de bewaarplicht wel het geval. Ervan uitgaan dat iedereen in de toekomst een strafbaar feit kan gaan plegen en dus bij voorbaat verdacht is, maakt de inbreuk onevenredig. ■

Aanbeveling

Breng het conceptwetsvoorstel tot aanpassing van de bewaarplicht telecommunicatiegegevens in overeenstemming met de internationale normen over privacybescherming.

Grondwet gaat moderne communicatie beschermen

Nu beschermt artikel 13 van de Grondwet alleen het ‘brief-, telefoon- en telegraafgeheim’. De overheid mag alleen brieven openen en telefoons aftappen als dat in de wet is geregeld. Voor het openen van een brief is een rechterlijke machtiging nodig. De Grondwet is op dit punt verouderd. Er staat niets in over nieuwe communicatiemiddelen als e-mail, chat of Skype. Het wetsvoorstel tot wijziging van artikel 13 van de Grondwet dat op 17 juni 2014 bij de Tweede Kamer is ingediend, beoogt de bescherming van privacy uit te breiden tot alle moderne telecommunicatiemiddelen. Een belangrijke stap vooruit. ■

De bescherming zou nog steviger moeten

Het wetsvoorstel bepaalt dat een rechterlijke machtiging niet nodig is voor het onderscheppen van een bericht, brief of e-mail als de nationale veiligheid in het gedrang is. Voorafgaande rechterlijke toetsing is echter ook in die situatie belangrijk, omdat de onafhankelijke rechter dan het privacybelang van de burger enerzijds, en het belang van de overheid om hierop een inbreuk te maken anderzijds, per geval kan afwegen. Is de voorgenomen maatregel noodzakelijk en proportioneel, gelet op het doel ervan? Bij toetsing achteraf kan het kwaad al geschied zijn.

Minister Plasterk stelt dat voorafgaande rechterlijke toetsing niet te rijmen valt met het karakter van de data-onderscheppingsoperaties door inlichtingen- en veiligheidsdiensten. Aangezien door dit soort operaties ook de relaties met andere landen (kunnen) raken, moet de verantwoordelijkheid voor het verlenen van toestemming bij de minister liggen en niet bij de rechter. Bovendien zou het volgens hem soms kunnen gaan om operaties buiten Nederlands grondgebied, zodat een Nederlandse rechter bij het verlenen van toestemming op problemen met de rechtsmacht zou kunnen stuiten. Deze argumenten overtuigen niet, alleen al omdat in het buitenland (bijvoorbeeld in de Verenigde Staten) wel in voorafgaande rechterlijke controle op dit type data-onderscheppingsoperaties is voorzien. Het College benadrukt daarom opnieuw zijn aanbeveling in de Jaarrapportage 2013. ■

Aanbeveling

Voorzie bij een inbreuk op het telecommunicatiegeheim in alle gevallen in voorafgaande rechterlijke toetsing.

Veiligheidsdiensten mogen straks ook ‘de kabel’ onderscheppen

In november 2014 heeft het kabinet een wijziging van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002) aangekondigd. De veiligheidsdiensten krijgen daarmee de bevoegdheid ook op de kabel ongericht informatie te onderscheppen. Zij kunnen dan grote hoeveelheden ruwe informatie ‘in de bulk’ onderzoeken. De huidige wet staat dat uitsluitend toe voor de ether en het draadloze telefonienetwerk. De Wiv 2002 is op dit punt achterhaald omdat 90% van de telecommunicatie, zoals internet en e-mail, tegenwoordig via de kabel gaat. De aanpassing van de wet volgt op een aanbeveling van de Commissie Dessens die in 2014 de Wiv 2002 evalueerde. ■

Niet de minister maar de rechter zou vooraf toestemming moeten geven

Het wetsvoorstel voorziet in toestemming door de minister voordat veiligheidsdiensten grootscheeps telecommunicatie mogen onderscheppen en onderzoeken. Het kabinet vindt dat daar de verantwoordelijkheid behoort te liggen vanwege het internationale aspect van de taakuitvoering van de veiligheidsdiensten. De verantwoordelijkheid voor de daaruit voortvloeiende mogelijke risico’s in alle gevallen moet worden gedragen door de minister en niet door de rechter. Het gaat hier echter om grootschalige data-onderscheppingsoperaties die mogelijk grote groepen mensen kunnen raken. Daarom heeft voorafgaande toetsing door een onafhankelijke instantie – een rechter of eventueel een onafhankelijke toezichthouder die bindende beslissingen kan nemen – de voorkeur; het is een betere garantie voor de weging van de verschillende belangen en het oordeel over de noodzaak, subsidiariteit en proportionaliteit van een dergelijke operatie. ■

Wel onafhankelijke toetsing bij onderschepping telecommunicatie journalisten

In zijn uitspraak in Telegraaf t. Nederland verwijst het EHRM naar eerdere jurisprudentie over toezicht door veiligheidsdiensten. Op terreinen waar misbruik van bevoegdheden zich gemakkelijk kan voordoen en er nadelige gevolgen voor de democratische samenleving kunnen zijn, heeft rechterlijk toezicht de voorkeur. Toetsing door andere instanties kan acceptabel zijn. Dan moet in ieder geval aan de eis van onafhankelijkheid zijn voldaan. Toetsing vooraf is vooral van belang omdat het onmogelijk is onthullingen van informatie ongedaan te maken. Het Kabinet heeft op deze EHRM-uitspraak gereageerd door een wetsvoorstel aan de Tweede Kamer voor te leggen dat erin voorziet om onderschepping van telecommunicatie door inlichtingen- en veiligheidsdiensten die erop gericht is om de bronnen van een journalist te achterhalen afhankelijk te maken van voorafgaande rechterlijke toestemming.

Ook in andere situaties, waarbij geen journalisten betrokken zijn, is die voorafgaande toetsing door een rechter of een onafhankelijke toezichthouder echter een belangrijke waarborg. ■

Interview

Aroosa (31), verhuisde op haar twaalfde vanuit Pakistan naar Nederland. Hier voelt Aroosa zich thuis. “Ik voel mij hier vrij en veilig. Er zijn wel momenten in mijn leven dat ik mij anders voelde, bijvoorbeeld in mijn studietijd. Het was voor mij nieuw dat mensen niet met mij samen wilden werken, omdat ik anders zou zijn. Terwijl ik niet het idee heb dat ik anders ben dan de ‘gewone’ Nederlander.”

In 2011 ging Aroosa op studiereis naar Israël. Wat een bijzondere reis moest zijn begon onprettig. “We kwamen eigenlijk heel vrolijk op Schiphol aan met de groep. In het begin kreeg iedereen simpele vragen; waarom ga je daar naartoe, etc. Maar alleen bij de niet-blanke mensen bleven ze doorvragen totdat ze wisten wat onze ‘roots’ zijn.”

Door middel van een risicoanalyse zijn Aroosa en vier andere studenten nader onderzocht door de luchtvaartmaatschappij. Alleen zij kregen persoonlijke vragen, de medewerkers controleerden hun bagage en ze werden expliciet gefouilleerd. “Achteraf vind ik wel dat mijn privacy geschonden is. Veiligheid is heel belangrijk, en dat moet voor iedereen gelden. Ik zou het ook erg vinden als ik met een mogelijke terrorist in een vliegtuig zit. Maar dat betekent niet dat je alleen de gekleurde mensen als potentieel gevaar mag aanduiden. Dat vind ik wel heel erg.

Aroosa kwam met haar klacht bij het College voor de Rechten van de Mens, die oordeelde dat zij gediscrimineerd is. Ze is blij met de uitspraak. “Die erkenning, dat was een heel belangrijk moment. Het gaf emotionele rust, dat wij in Nederland een systeem hebben dat je ook als individu beschermt. Er moet geen systeem zijn wat voor de één wel goed is, maar voor een ander niet.” Aroosa vindt het wel kwalijk dat dit in Nederland kan gebeuren. En de luchtvaartmaatschappij bood ook nooit haar excuses hiervoor aan. “Toen ik hulp zocht werd er veel tegen mij gezegd; dit is de realiteit, accepteer het maar. Daar moet verandering in komen, dat je het oké vindt dat vijf van de veertien studenten anders worden behandeld.”

Bindend oordeel op rechtmatig optreden veiligheidsdiensten is cruciaal

In Nederland is toezicht op de veiligheidsdiensten in handen van de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD).
Het College deed in zijn Jaarrapportage 2013 de aanbeveling om dit toezicht te versterken door de oordelen van de CTIVD juridisch bindend te maken en bij grootschalige data onderschepping te voorzien in voorafgaande of versnelde rechtmatigheidscontrole.

Het kabinet wijst het juridisch bindend maken van het rechtmatigheidsoordeel van de CTIVD af met wel een snelle maar niet bindende toetsing door de CTIVD; het kabinet wil ruimte laten voor de mogelijkheid dat de minister een door de CTIVD als onrechtmatig beoordeelde praktijk toch doorzet. Het College wijst erop dat het kabinet hiermee een essentieel onderdeel van de aanbevelingen van de Commissie Dessens negeert. Juist met het oog op de uitbreiding van de data-onderscheppingsbevoegdheden van de veiligheidsdiensten beval deze immers aan de toezichtfunctie van de CTIVD te versterken en deze daarbij de bevoegdheid toe te kennen tot het geven van een bindend rechtmatigheidsoordeel. De jurisprudentie van het EHRM laat zien dat het Hof van oordeel is dat een rechterlijke goedkeuring vooraf de beste waarborgen biedt.
Als die er niet is, dan is het noodzakelijk dat de toetsing achteraf met zeer sterke waarborgen is omkleed, zoals de mogelijkheid bindende oordelen te geven. Juist vanwege het massale karakter van ongerichte informatieonderschepping mag die mogelijkheid niet beperkt zijn tot het geven van een bindend oordeel op – sporadisch – ingediende klachten. ■

Aanbeveling

Het College specificeert zijn aanbeveling uit 2013: Versterk het onafhankelijk toezicht op de inlichtingen- en veiligheidsdiensten door bij grootschalige data-onderschepping te voorzien in voorafgaande of versnelde – en bindende – rechtmatigheidscontrole door de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD). Beperk het bindend karakter van de CTIVD-toetsing niet tot de oordelen in klachtprocedures.

Er komen voorwaarden voor samenwerking met andere landen

Het kabinet heeft besloten een aantal waarborgen en criteria voor de samenwerking met andere landen op te nemen in de Wiv 2002. Ten eerste is altijd toestemming van de minister nodig voordat veiligheidsdiensten grootscheeps informatie in de bulk mogen uitwisselen met buitenlandse veiligheidsdiensten. Ten tweede komen er criteria in de wet waaraan een land moet voldoen waarmee een dienst wil gaan samenwerken. Deze criteria zijn de democratische inbedding van de dienst, het mensenrechtenbeleid in het desbetreffende land en de professionaliteit en betrouwbaarheid van de dienst. Als een land en/of dienst onvoldoende aan deze criteria voldoen, moet de minister beslissen of en zo ja, wat de aard en intensiteit van de samenwerking kan zijn.

Een criterium dat nog toevoeging verdient, is het naar behoren functioneren van het rechtmatigheidstoezicht op de veiligheidsdiensten in het desbetreffende land. Ook beveelt het College aan in het wetsvoorstel nauwkeurig te omschrijven wie bepaalt of een land aan de genoemde criteria voldoet en welke procedure daarbij wordt gevolgd. ■

Aanbeveling

Neem in de Wiv 2002 als voorwaarde voor samenwerking met een buitenlandse veiligheidsdienst op dat bij die dienst is voorzien in adequaat rechtmatigheidstoezicht en leg in die wet expliciet vast wie bepaalt wanneer voldaan is aan de wettelijke afwegingscriteria voor samenwerking met andere landen.