

Ministerie van Veiligheid en Justitie
t.a.v. de heer mr. dr. K.H.D.M. Dijkhoff
Postbus 20301
2500 EH DEN HAAG

Den Haag, 10 juli 2017
dossiernummer: 103685
uw kenmerk: 2068042
telefoonnummer: +31 (0)70 335 35 65
e-mail: e.vandenbosch@advocatenorde.nl

Betreft: ontwerpbesluit onderzoek in een geautomatiseerd werk

Geachte staatssecretaris,

Bij brief van 10 mei 2017 heeft u de Nederlandse orde van advocaten (NOvA) ter consultatie voorgelegd het ontwerpbesluit onderzoek in een geautomatiseerd werk. De NOvA voldoet graag aan uw verzoek en heeft zijn adviescommissie strafrecht gevraagd te adviseren.

Bijgaand stuur ik u het advies van de adviescommissie. De algemene raad sluit zich aan bij de overwegingen van de adviescommissie en verzoekt u deze bij de verdere uitwerking te betrekken.

Met de meeste hoogachting,
namens de algemene raad,



mw. mr. R.G. van den Berg
algemeen secretaris

bijlage: advies van de adviescommissie

Bezoekadres
Neuhuyskade 94
2596 XM Den Haag
Tel. 070 - 335 35 35
Fax 070 - 335 35 31

Postadres
Postbus 30851
2500 GW Den Haag

ADVIES

Van	: adviescommissie strafrecht
Datum	: 10 juli 2017
Betreft	: Besluit onderzoek in een geautomatiseerd werk

I. Inleiding

1. Het ter consultatie voorgelegde Besluit werkt het Wetsvoorstel Computercriminaliteit III nader uit. Op dit wetsvoorstel is vanuit het maatschappelijk veld uitgebreid en steeds zeer kritisch gereageerd. Net als anderen stelde de NOvA eerder vast dat een 'zeer ingrijpende en verregaande opsporingsbevoegdheid' werd gecreëerd, die fundamentele problemen openliet. Het wetsvoorstel ligt thans voor in de Eerste Kamer, waar het (wederom) veel vragen van maatschappelijke, praktische en juridisch aard oproept. De NOvA blijft bij het standpunt dat het wetsvoorstel gezien de redenen die het eerder naar voren bracht niet tot wet zou moeten worden verheven.
2. Het huidig Advies ziet niet op het wetsvoorstel zelf maar (slechts) op het Besluit dat aan dit wetsvoorstel uitvoering zou moeten geven. Daartoe bespreekt het eerst het voorstel (Besluit) in het licht van EVRM verplichtingen. Daarna wordt ingegaan op de betrouwbaarheid van datavergaring en de mogelijkheid om die betrouwbaarheid te testen. Tot slot wordt de uitbreiding van het aantal misdrijven waarbij de bevoegdheden kunnen worden ingezet besproken.

II. Het voorstel in het licht van EVRM verplichtingen

3. Omdat het voorstel zeer invasieve inbreuken op de persoonlijke levenssfeer (zoals beschermd door artikel 8 EVRM) regelt stelt het EHRM significante eisen aan de kwaliteit van deze wet. Deze moet adequate waarborgen bieden tegen misbruik, door voldoende specifiek, duidelijk en toegankelijk te zijn. Verscheidene verdragspartijen bij het EHRM zijn inzake het ontbreken van kwalitatief voldoende wetgeving op de spreekwoordelijke vingers getikt. Zo voldeed de Britse wet die de onderschepping van communicatie door het Britse ministerie van defensie er niet aan (uitspraak van 2008).¹ Hetzelfde gold voor de Russische wet (2015)², de Hongaarse wet (2016)³, de Kroatische wet (2015)⁴, de Franse wet (1990)⁵ en de Zwitserse wet (2000)⁶.
4. De volgende uitspraken zijn, in het licht van het huidig voorstel, in het bijzonder noemenswaardig. In de zaak tegen Hongarije⁷ achtte het EHRM in het bijzonder problematisch dat hoeveelheden data werden onderschept die buiten het bereik van de oorspronkelijke onderzoek vielen. Dit is typisch wat in Nederland ook zal plaatsvinden en waar het voorstel onvoldoende waarborgen voor bevat. Immers, de Staat breekt in op een computer of enig ander digitaal apparaat die bij verschillende personen in gebruik kan zijn.

¹ Liberty cs. tegen het Verenigd Koninkrijk, 1 juli 2008.

² Roman Zakharov tegen Rusland, 4 december 2015.

³ Szabó en Vissy tegen Hongarije, 12 januari 2016.

⁴ Dragojević tegen Kroatie, 15 januari 2015.

⁵ Kruslin tegen Frankrijk, 24 april 1990.

⁶ Amann tegen Zwitserland, 16 februari 2000.

⁷ Szabó en Vissy tegen Hongarije, 12 januari 2016.

Het voorstel stelt zelfs expliciet dat het doel van het inbreken kan zijn om vast te stellen welke personen van het apparaat gebruik maken. Waarborgen om inbreuken op de persoonlijke levenssfeer van personen die geen deel uitmaken van het onderzoek lijken niet goed wettelijk te zijn geregeld.

5. Daarnaast bekritiseerde het EHRM in de zaak tegen Hongarije dat de uitvoerende macht kon optreden zonder dat de strikte noodzakelijkheid van dit optreden vaststond. Dit klemde des te meer, nu een effectieve gerechtelijke toetsing leek te ontbreken. In het huidige voorstel speelt de Officier van Justitie (de uitvoerende macht) een cruciale rol. Het voorstel geeft aan dat de geobserveerde persoon eventuele problemen bij de zittingsrechter kan neerleggen. Daarbij merkt het expliciet op dat de geheimhouding van methoden en technieken reden kan zijn om slechts summier over de toegepaste techniek te verklaren en dat de zittingsrechter buiten de persoon om (dus onder geheimhouding) aan de opsporingsdiensten vragen kan stellen. Hier komt bij dat lang niet iedere toepassing van bevoegdheden aan een zittingsrechter wordt voorgelegd. Wanneer niet tot vervolging wordt overgegaan of wanneer de Officier van Justitie de verkregen informatie niet relevant acht voor de strafzaak (en dus de informatie niet aan het dossier toevoegt) zal de geobserveerde persoon in feite zonder effectief rechtsmiddel blijven. Kortom, regelmatig zal de inzet van bevoegdheden niet door de geobserveerde getoetst kunnen worden en wanneer hij dat wel kan, dan is de toetsing beperkt.
6. In EHRM Roman Zakharov tegen Rusland⁸ achtte het EHRM de Russische wet in strijd met artikel 8 EVRM op tal van terreinen. Een aantal hiervan zijn hierboven al genoemd en behoeven geen herhaling. Een van de problemen lag in het feit dat men alleen kon klagen over de inzet van bevoegdheden wanneer de klager bewijs kon leveren van het feit dat bevoegdheden ook daadwerkelijk waren ingezet jegens hem. Zulk bewijs was evenwel praktisch onmogelijk om te leveren. Ook hier loopt weer een parallel met Nederland. Zoals eerder aangegeven zal alleen wanneer tot strafvervolging wordt overgegaan en de verkregen informatie aan het dossier wordt toegevoegd de inzet van bevoegdheden bekend worden. Dit dekt lang niet alle gevallen en sluit in ieder geval personen die als 'bijvangst' gelden uit. Bijvangst zijn personen over wie wel informatie wordt vergaard (bijvoorbeeld doordat zij dezelfde computer gebruiken als de verdachte) maar tegen wie geen procedure aanhangig wordt gemaakt. Het voorstel voorziet niet in informatieverstrekking aan personen dat in hun rechten onder artikel 8 EVRM is getreden. Dit maakt dat de overheid, mogelijk in strijd met het EVRM, zeer indringende informatie kan vergaren en verwerken over personen zonder dat deze personen hier weet van hebben of zich hiertegen kunnen verzetten.
7. In dit laatste kader zijn twee zaken tegen respectievelijk Frankrijk⁹ en Zwitserland¹⁰ noemenswaardig. Brunet tegen Frankrijk (2014) ging over een klager tegen wie een onderzoek had gelopen dat daarna werd afgebroken. Gegevens uit dat onderzoek werden evenwel aan een politiedatabank toegevoegd. Het EHRM oordeelde dat het bewaren van de gegevens een disproportionele inbreuk op klagers recht op privéleven inhield, die in een democratische samenleving niet noodzakelijk was. In het bijzonder overwoog het Hof dat klager geen praktische mogelijkheid ten dienste stond om de informatie verwijderd te krijgen en de informatie lang – en wellicht zelfs oneindig – bewaard kon worden. Het thans voorliggende voorstel voorziet weliswaar in de vernietiging van informatie na afloop van de

⁸ Roman Zakharov tegen Rusland, 4 december 2015.

⁹ Brunet tegen Frankrijk, 18 september 2014.

¹⁰ Khelili tegen Zwitserland, 18 oktober 2011.

strafzaak en wanneer tot sepot is besloten. Echter, dit gaat over de 'ruwe' data en de vraag komt op of dit ook betekent dat verwerkte data (opsporingsdiensten verwerken data vaak bijvoorbeeld om zicht te krijgen op netwerken¹¹ – een doel waar het voorstel ook naar verwijst) wordt verwijderd. Ten minste net zo belangrijk is dat lang niet ieder onderzoek eindigt in strafvervolgning of sepot. Wanneer de zaak niet is 'opgelost' gaat het onderzoek – zoals de toelichting bij het voorstel ook toegeeft – op een laag pitje door. Dit betekent dat alle in het onderzoek verzamelde gegevens tot de verjaringstermijn (decennia en soms nooit) van het onderzochte feit bewaard blijven, zonder dat een effectieve mogelijkheid van verwijdering bestaat. Dit kan goed in strijd komen met het bepaalde in Brunet tegen Frankrijk.

8. De zaak *Khelili tegen Switzerland* (2011) voegt hier nog aan toe dat het al dan niet automatisch verwerken van de verkregen gegevens meeweegt bij de vraag of van een inbreuk op het recht op privéleven sprake is. Inherent aan digitaal verkregen gegevens is dat zij gemakkelijk gedeeld en verwerkt kunnen worden. Nu voorziet de wet reeds in verwerking.¹² Het is zorgwekkend dat het besluit niets stelt over automatische verwerking en de noodzaak om dit nu en in de toekomst te beperken.¹³
9. Eveneens maakt EHRM jurisprudentie duidelijk dat de inzet van specifieke onderzoeksmiddelen die inbreuk maken op het privéleven ook specifieke wetgeving vereist. Met het binnendringen van geautomatiseerde werken kunnen verschillende functies van die werken worden overgenomen, zoals transcriptie, geluidsopname en het vastleggen van bewegend beeld. In *Vettel tegen Frankrijk* plaatste opsporingsautoriteiten afluisterapparatuur in de flat van een moordverdachte. De Franse wet regelde echter niet specifiek ten aanzien van afluisterapparatuur hoe deze diende te worden ingezet, waarna een schending vaststond.¹⁴ Hetzelfde overkwam twee jaar eerder het Verenigd Koninkrijk, waar video-opnames werden gemaakt zonder voldoende specifieke wettelijke basis om te beschermen tegen misbruik.¹⁵ Noch de voorgestelde wet computercriminaliteit II, noch het voorliggende voorstel splitsen uit naar functie en voorzien in specifieke, op die functie toegesneden waarborgen.
10. Wat verder opvalt aan het voorstel is dat het niet regelt wanneer mag worden binnengedrongen in gevallen waarin onbekend is waar informatie is opgeslagen. Zulke gevallen zijn hoogst gevoelig; in de kern gaat het om datavergaring bij (onder meer) personen die niet aan enig strafbaar handelen gelinkt kunnen worden, maar via wie men mogelijkwijs bij opgeslagen gegevens kan komen. Het wetsvoorstel biedt de Minister de mogelijkheid om deze bevoegdheid per AMvB uit te werken. De uitwerking wordt volgens de toelichting echter overgelaten aan het College van procureurs-generaal, dat een Aanwijzing zal opstellen. Dit illustreert het algemene probleem met het wetsvoorstel en het besluit,

¹¹ Zie artikelen 8-14 Wet Politiegegevens.

¹² Zie artikelen 8-14 Wet Politiegegevens.

¹³ Zie *S. en Marper tegen het Verenigd Koninkrijk*, 4 december 2008, § 103: *"The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article ... The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored ... [It] must also afford adequate guarantees that retained personal data were efficiently protected from misuse and abuse ..."*

¹⁴ *Vetter tegen Frankrijk*, 31 mei 2005.

¹⁵ *Perry tegen het Verenigd Koninkrijk*, 17 juli 2003.

namelijk dat het controversiële en ingrijpende inbreuken op burgerrechten het liefst niet in de wet vastlegt, maar onder de Minister houdt die zich dan (enkel?) door de top van het opsporingsapparaat laat leiden. Ook hier geldt weer dat aan het EVRM vereiste van voorzien en kenbaar bij wet goed niet voldaan kan zijn.

III. Betrouwbaarheid van het middel en controle op die betrouwbaarheid

11. Deskundigen hebben vaak gewaarschuwd dat het wetsvoorstel de digitale veiligheid aantast. Binnendringen kan namelijk de veiligheid van het systeem waarin is binnengedrongen verzwakken. Tevens behoudt de overheid zich het recht voor om gaten in de beveiliging waar het zelf gebruik van maakt niet te melden, zodat de gaten voor kwaadwillenden over de gehele wereld beschikbaar blijven. Ook is verre van zeker dat de overheid niet zelf veiligheidsproblemen zal ondervinden. Het Besluit lijkt weinig aan deze bezwaren te doen. Sterker, het lijkt deze bezwaren te negeren. Zo zou herkeuring van een middel slechts behoeven plaats te vinden wanneer het middel significant (door de overheid zelf) is aangepast (zodat er de facto sprake is van een nieuw middel). Dit betekent dat zolang een middel maar niet wordt aangepast (in ICT-termen: ge'upgrade) het eeuwig voor veilig en betrouwbaar wordt gehouden. In periodieke toetsing voorziet het Besluit niet. Dit tast de betrouwbaarheid en integriteit van de middelen aan. Dit extra bezwarend, nu het wetsvoorstel en het besluit niet voorzien in een voldoende effectieve controle op de betrouwbaarheid.
12. Ter illustratie van het bovenstaande een (fictief) voorbeeld. In 2018 wordt een middel goedgekeurd op criteria zoals betrouwbaarheid en veiligheid. Goedgekeurd betekent ook dat goedkeuring al eens is verleend in een EU land of middels Verdrag – dan wordt geen eigen keuring meer uitgevoerd. Als geen buitenlandse goedkeuring beschikbaar is kan de keuring worden uitgevoerd door een private partij, die met een Keuringsprotocol moet werken. Noodzakelijkerwijs verkeert die partij in een afhankelijke positie ten opzichte van zijn opdrachtgever (de overheid). Met het op deze wijze goedgekeurde middel in de hand wordt vervolgens binnengetrepen en informatie verkregen. Deze moet zijn weg vinden naar het strafproces. Volgens de toelichting op het Besluit

'zal in het proces-verbaal van de inzet worden verwezen naar het keuringsnummer, waardoor de samenstelling van het hulpmiddel ter bescherming van de opsporingsbelangen, kan worden afgeschermd.

Indien tijdens de behandeling van een strafzaak twijfels zouden rijzen over de betrouwbaarheid en de integriteit van het tijdens het onderzoek vergaarde bewijs, kan de rechter de volledige informatie opvragen of een deskundige raadplegen. Hierbij staat de rechter de procedure zoals omschreven in artikel 187d Sv ter beschikking, waarin de rechter-commissaris kan beletten dat antwoorden op vragen ter kennis komen van de verdachte en diens raadsman, indien er een gegrond vermoeden bestaat dat door de openbaarmaking een zwaarwegend opsporingsbelang wordt geschaad.¹⁶

13. Verplaatsen wij ons naar de positie van de verdachte die de betrouwbaarheid en de integriteit van het bewijs (de door de overheid gepresenteerde informatie) betwist. Meer dan

¹⁶ Toelichting, par. 3.4.

dat die informatie onjuist of onvolledig is kan zij niet stellen. Zij weet ook niet welke informatie nog meer beschikbaar is; de 'samenstelling van het hulpmiddel' is immers afgeschermd en daarnaast heeft (conform het Besluit) de recherche-afdeling die zich met binnendringen bezighoudt aan de OvJ alleen informatie doorgegeven die binnen het bevel leek te passen. De verdachte kan de rechter dus niet uitleggen waarom de informatie niet klopt, noch welke informatie zij zou willen hebben. Aan de hand van het keuringsnummer kan zij enkel nagaan dat het middel waarmee het verkregen is op enig moment en ergens betrouwbaar is bevonden. Voor haar is het aldus volstrekt onmogelijk om effectief de betrouwbaar en integriteit van de informatie die haar wordt tegengeworpen na te gaan, laat staan te betwisten. Tevens heeft zij weinig in handen om de rechter te overtuigen dat een deskundige dient te worden aangesteld. Immers, dit behoeft een gedegen motivering en aldus een stuk meer dan de 'die informatie klopt niet' dat zij naar voren kan brengen.

14. Wanneer desalniettemin vervolgens een deskundige aangesteld zou worden, dan zouden volgens de Minister opsporingsbelangen een grote rol moeten spelen. Opsporingsbelangen zijn een synoniem voor geheimhouding. Dit beperkt de mogelijkheid om vragen te stellen en aldus tot een serieuze toetsing te komen. Daarbij hangen de kwaliteit van antwoorden nauw samen met de kwaliteit van de vragen; zonder gedegen kennis en begrip van het middel is het moeilijk, zo niet onmogelijk, om de juiste vragen te stellen. Een rechter kan hier niet voor compenseren; hij kent het leven van de verdachte niet en kan zich dus alleen op algemeenheden baseren; er is een reden dat de verdediging bij het verhoor van een deskundige vrijwel altijd een significante rol heeft. Een rol die daarbij gegrondvest is op het in artikel 6 EVRM opgenomen recht om bewijs effectief te kunnen betwisten. Het voorstel komt hier niet aan tegemoet.

IV. Uitbreiding categorie van misdrijven

15. Volgens het wetsvoorstel kan de Minister ieder strafbaar feit bij AMvB aanwijzen als geschikt voor de toepassing van de bevoegdheden. In de Memorie van Toelichting wordt hierover het volgende geschreven:

"De bij algemene maatregel van bestuur aan te wijzen misdrijven betreffen misdrijven waarop weliswaar geen gevangenisstraf van acht jaar of meer is gesteld maar die worden gepleegd met behulp van een geautomatiseerd werk en waarbij er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders. Er is dan vaak geen ander aangrijpingspunt voor de opsporing. Dit betreft misdrijven als het gebruik van een botnet (artikel 138ab, derde lid, Sr), het aanbieden, verspreiden of bezitten van kinderpornografie (artikel 240b Sr), de verleiding van een minderjarige tot ontucht (artikel 248a Sr) de «grooming» (artikel 248e Sr) of andere ernstige delicten waarbij het gebruik van een geautomatiseerd werk instrumenteel is en de inzet van deze bevoegdheid op basis van een afweging van belangen en met inachtneming van de proportionaliteit en subsidiariteit aangewezen is."¹⁷

16. De door de wetgever geboden garantie dat toepassing beperkt zal blijven tot "*ernstige delicten waarbij het gebruik van een geautomatiseerd werk instrumenteel is*" wordt door het voorliggende besluit nu reeds teniet gedaan. Immers, aangewezen worden onder meer het

¹⁷ MvT, Kamerstukken II, 34372, nr. 3, p. 29.

deelnemen aan een criminele organisatie (art. 140 Sr), corruptie (art. 177, 179, 182 en 200 Sr), fraude (art. 225, 226, 227, 231, 231a en 232 Sr) en witwassen (art. 420bis Sr). Daarbij stelt het besluit nadrukkelijk niet de eis dat de bevoegdheden alleen kunnen worden ingezet wanneer bij het onderzochte delict "*het gebruik van een geautomatiseerd werk instrumenteel is*".

17. Een vermoeden van witwassen ontstaat snel. Immers, witwassen omvat onder andere het voorhanden hebben, gebruik maken of omzetten van geld of goederen, waarvan aannemelijk is dat deze uit enig misdrijf zijn verkregen. Het is feitelijk aan de verdachte om (later) aan te tonen dat het geld of de goederen wel degelijk een legale herkomst hadden. Het bezit van contante geldbedragen (soms al zo weinig als duizend euro) of gebruikmaken van inkomsten van de partner leiden in de praktijk gemakkelijk tot veroordelingen voor witwassen.¹⁸ De eenvoudige werkelijkheid is dat een paar keer goed uit eten zonder dat bij Justitie een hoog inkomen bekend is een vermoeden van witwassen oplevert, waarna de inzet van zeer ingrijpende bevoegdheden mogelijk wordt – zoals het veranderen van de telefoon van de betrokkene in een opname- en transcriptieapparaat.
18. De inzet van het besluit is niet alleen het reguliere strafrecht maar ook fiscale delicten. De toelichting bij het besluit stelt (nu al) dat bij "*de FIOD/ECD bestaat behoefte aan deze bevoegdheid met het oog op de strafrechtelijke handhaving van de rechtsorde op bepaalde beleidsterreinen*". Dit brengt fiscale delicten via de achterdeur van het witwassen / de criminele organisatie expliciet onder de reikwijdte van de hackbevoegdheid.
19. Met dit in het achterhoofd worden de waarborgen die de EVRM jurisprudentie op artikel 8 EVRM eist door de adviescommissie nagelopen. Ten eerste de eis dat de categorie van misdrijven waarbij bevoegdheden worden uitgeoefend beperkt dient te zijn. Dit is van belang in het kader van de proportionaliteit en de subsidiariteit. Dat het wetsvoorstel zeer diep ingrijpt in het onder artikel 8 EVRM beschermde privéleven van burgers behoeft geen betoog. Noch het wetsvoorstel, noch het besluit, waarborgen die proportionaliteit. Immers, nu al wordt witwassen zonder meer aangewezen als delict waarvoor de bevoegdheden kunnen worden toegepast, wat de surveillance van ieder persoon met niet onmiddellijk verklaarbaar bezit toelaat.
20. Overigens is dit voor de opsporingsinstanties een buitenkans om als 'bijvangst' de rest van het leven van een persoon in wie interesse is in kaart te brengen. Nu al is het waar mogelijk standaard praktijk om naast een 'grondmisdrijf' (het misdrijf waar werkelijke interesse naar uitgaat) ook witwassen ten laste te leggen, omdat bij dit laatste de bewijsstandaarden aanzienlijk lager zijn. Het OM maakt er geen geheim van dat dit is zodat als het misdrijf niet kan worden bewezen, dan in ieder geval wel het geld gepakt kan worden. Weinig houdt het OM dan ook tegen om op basis van het wetsvoorstel en besluit het witwassen als haak voor de opsporing en bestraffing van allerhande verdenkingen te gaan gebruiken.
21. Daarnaast staat het de Minister vrij om later, nadat het voorstel wet zou zijn geworden, meer delicten toe te voegen. Verwacht mag worden dat de waan van de dag, politieke motieven (kracht of aandacht uitstralen) en de overheid kenmerkende controledrang zullen leiden tot een steeds uitdijende lijst aan delicten waarbij de hier besproken bevoegdheden worden

¹⁸ Zie bijvoorbeeld de uitspraak van de Hoge Raad van 16 april 2013 (ECLI:NL:HR:2013:BZ7149) waar de verdachte gebruik maakte van de auto van haar partner, terwijl zij had moeten weten dat deze partner onvoldoende (legale) inkomsten had om deze auto te kunnen bekostigen.

ingezet. Dat delicten ook weer van de lijst zullen worden afgevoerd is niet aannemelijk, omdat (anders dan bij toevoegen) daar nooit een direct belang bij is. Kortom, het thans voorliggende besluit maakt de ruime toepassing van zeer indringende opsporing nu al mogelijk, waarbij die toepassing later kan (en zal) worden uitgebreid. Het is dan ook dringend noodzakelijk dat wettelijk (op het niveau van het parlement) wordt vastgelegd bij verdenking van welke misdrijven inzet gepast kan zijn. Dit waarborgt niet alleen de noodzakelijke democratische controle, maar ook de bescherming van individuele rechten.