NEDERLANDSE ORDE VAN ADVOCATEN

Advies

inzake

het wetsvoorstel

Wijziging van het Wetboek Strafvordering in verband het gebruik van elektronische processtukken (digitale processtukken)

1. Inleiding

1.1 Het wetsvoorstel digitale processtukken beoogt het gebruik van digitale processtukken in de strafrechtspleging te faciliteren en te kanaliseren.

1.2 Meer specifiek strekt het wetsvoorstel tot introductie van een drietal nieuwe regelingen in het Wetboek van Strafvordering:

1. Een regeling voor de integriteit van processtukken in elektronische vorm;
2. Een regeling voor het elektronisch ondertekenen van processtukken; en
3. Een regeling voor de elektronische overdracht van processtukken.

1.3 Algemeen bezien juicht de Adviescommissie Strafrecht (ACS) een digitalisering van het strafproces toe. In zoverre staat zij dan ook positief tegenover het beproeven van de mogelijkheden van de techniek en de wens om processtukken te digitaliseren en het indienen van verzoekschriften en klaagschriften en alle andere stukken digitaal mogelijk te maken.

1.4 Een en ander betekent evenwel niet dat de beoordeling van het wetsvoorstel zonder kritiek blijft. Vanuit het perspectief van rechtsbescherming van diegenen die (meestal ongewild) aan een strafproces worden onderworpen (verdachten, veroordeelden, slachtoffers, aangevers en getuigen) kunnen samengevat de volgende aanbevelingen worden gedaan:

- Het scheppen van duidelijkheid over de groep justitiabelen waarop deze nieuwe regels betrekking zullen hebben (4.8)
- Nader te omschrijven wat bedoeld wordt met de mogelijke verstrekking via “DigID midden” (4.9)
- De mogelijkheid tot aanlevering van procesdossiers aan de verdediging op USB-stick, CD-Rom te laten blijven bestaan (4.11)
- De verkrijging van toegang tot digitale gegevens en de onbelemmerde mogelijkheid tot het doen van aangifte en aanwenden van rechtsmiddelen door gedetineerden nader te regelen en garanderen (4.12, 4.20 en 4.23-4.25))
- Aan te geven om welke uitzonderingen het gaat bij de vernietiging van papieren dossiers ‘behoudens uitzondering’ (4.13-4.16)
- Nadere regels te stellen omtrent de beveiligde opslag van gegevens na ontvangst daarvan (4.17 – 4.18)
- De wijze van instellen van een rechtsmiddel in geval van een strafbeschikking aan die van andere situaties waarbij een rechtsmiddel wordt ingesteld gelijk te maken (4.25).

2. De integriteit van processtukken in elektronische vorm

2.1 Op p. 19 en 20 van de concept Memorie van Toelichting (MvT) wordt nader ingegaan op de voorgestelde regeling voor de integriteit van processtukken in elektronische vorm (paragraaf 2.1).

2.2 Met het begrip *"integriteit"* wordt in de MvT gedoeld op de zekerheid dat het document volledig is en niet onbevoegdelijk is gewijzigd. Derhalve zullen van het digitale document gegevens moeten worden vastgelegd, zoals de auteur, de datum en tijdstip van het opstellen en het aanbrengen van wijzigen. Ook zal verifieerbaar sprake moeten zijn van een zogenoemde "unbroken custody" (ononderbroken beheer).

2.3 Volgens de MvT kan met een bepaalde techniek de integriteit van een elektronisch document worden gecontroleerd. Een veel gebruikte techniek is (kennelijk) het technisch tekenen van documenten. Bij technisch tekenen wordt de zogenoemde "hashwaarde" van het document berekend en versleuteld met een private sleutel van een certificaat. Bij een latere controle kan de hashwaarde worden vergeleken en kan worden gecontroleerd of het document tussentijds is gewijzigd.

2.4 In zoverre lijkt dit gewaarborgd. Er blijft evenwel ook nog veel onduidelijk. De MvT laat bijvoorbeeld onvermeld of ten aanzien van alle processtukken standaard een dergelijke controle zal worden uitgevoerd, en zo ja of de resultaten van die controle beschikbaar zullen zijn voor de procesdeelnemers zoals de verdachte en diens raadsman. Als de controle niet standaard wordt uitgevoerd, blijft onduidelijk hoe procesdeelnemers zoals de verdachte en diens raadsman er achter komen of de controle op een bepaald document is uitgevoerd en hoe zij kunnen bewerkstelligen dat deze controle alsnog wordt uitgevoerd (door henzelf of door Justitie).

3. Elektronisch ondertekenen van processtukken

3.1 Een regeling die met de genoemde integriteit direct samenhang is het digitaal waarmerken of ondertekenen van documenten. Dit onderwerp wordt in de MvT op p. 20-28 (paragraaf 2.2 en 2.3) behandeld.

3.2 De inhoud van deze paragraaf is vrij technisch. De ACS voelt zich onvoldoende geëquipeerd om dit wetsvoorstel ook op deze technische aspecten te kunnen beoordelen. Omdat dit wellicht voor meer betrokkenen bij dit wetsvoorstel geldt, adviseert de ACS om dit wetsvoorstel voor te leggen aan een onafhankelijke IT-deskundige.

4. Elektronische overdracht van processtukken

4.1 In paragraaf 3 van de MvT wordt de elektronische overdracht van processtukken behandeld. Deze overdracht wordt omschreven als het elektronisch verkeer tussen justitiabele (al dan niet door een rechtshulpverlener vertegenwoordigde verdachte, slachtoffer, getuige of getuige-deskundige) en de rechterlijke macht (zijnde de griffie, de rechter, het parket en de officier van justitie) (zie p. 32 MvT). De ACS vindt het enigszins verwarrend dat over "rechterlijke macht" wordt gesproken waarbij ook het Openbaar Ministerie is inbegrepen, maar dit ter zijde.

4.2 De ACS begrijpt dat de voorgestelde regeling van overdracht twee richtingen op werkt: ten eerste de informatieverstrekking *door* de overheid *aan* de bovengenoemde justitiabele en ten tweede de informatieverstrekking *aan* de overheid *door* de justitiabele. In de MvT is dit onderscheid niet (altijd) even duidelijk aangebracht.

Kennisgeving van het procesdossier

4.3 De verstrekking van het procesdossier *aan* de justitiabele, en dan met name de verdachte en diens advocaat, wordt behandeld in paragraaf 3.1 van de MvT (p. 33 e.v.). Interessant wordt het op pagina 35.

4.4 Het toeval wil dat de ACS van het Ministerie van Veiligheid en Justitie een versie van het conceptwetsvoorstel heeft toegezonden gekregen waarin de intern aangebrachte tekstwijzigingen met track changes zichtbaar zijn. Dit zal niet helemaal de bedoeling zijn geweest, maar is tegelijkertijd ook weer een goed voorbeeld hoe kwetsbaar digitale verstrekking kan zijn. Het baart, juist als het gaat om een wetsvoorstel als het onderhavige, enigszins zorgen over de omgang van de overheid met moderne technieken en maakt duidelijk dat de waarborgen voor een zorgvuldige omgang met de vertrouwelijke gegevens waarop het wetsvoorstel betrekking heeft, stevig verankerd moeten zijn in de wet.

4.5 Gedoeld wordt hier op pagina 35, waar kennelijk door de laatste auteur van de MvT een verwijzing is weggehaald naar de uitspraak die gepubliceerd is in "*NS* 2006/107". Uit die uitspraak blijkt dat door de officier van justitie (delen van) het procesdossier alleen digitaal aan de verdediging waren verstrekt. Op het verzoek van de verdediging om een papieren versie te kunnen ontvangen werd door de officier van justitie niet gereageerd. De rechtbank bepaalde vervolgens dat er geen wettelijk basis is voor het uitsluitend verstrekken van een digitaal procesdossier. Alleen als door alle procespartijen tevoren afspraken zijn gemaakt, zou volgens de rechtbank kunnen worden volstaan met verstrekking van een digitaal dossier.

4.6 Het is de ACS onduidelijk waarom deze verwijzing in de MvT is weggehaald. Het illustreert namelijk juist goed de problemen in de praktijk vanuit het perspectief van de verdediging: er moet niet alleen iets geregeld worden voor het verkeer tussen of aan overheden zoals het Openbaar Ministerie en rechterlijke macht, maar er is zeker ook behoefte aan duidelijke regels voor informatieverstrekking *door* de overheid *aan* de justitiabele.

4.7 In de MvT wordt in dat opzicht (slechts) opgemerkt dat in het Besluit processtukken in strafzaken regels zullen worden toegevoegd over het langs elektronische weg verstrekken van processtukken *"aan de verdachte of diens raadsman"*. Twee zinnen later wordt gesproken over de verstrekking aan "een verdachte of een slachtoffer" via "DigID midden".

4.8 Daarmee is er onduidelijkheid over de groep justitiabele waarop deze nieuwe regels betrekking zullen hebben. De ACS zou dan ook graag zien dat uit de tekst van de MvT duidelijk(er) naar voren komt dat zowel de verdachte, het slachtoffer in de zin van art. 51a Sv, de getuige, de getuige-deskundige alsmede diens advocaten binnen de regeling vallen.

4.9 Voorts is het de ACS volstrekt niet duidelijk wat bedoeld wordt met mogelijke verstrekking via *"DigID midden"*. Gelet op het praktische belang, zou enige tekst en uitleg wel aangewezen zijn. De ACS heeft op internet (www.digid.nl) het volgende gevonden:

Zekerheidsniveau Midden

Heeft u bij uw DigiD aanvraag, ook uw mobiele nummer opgegeven? Dan heeft u DigiD met sms-functie, oftewel zekerheidsniveau Midden. Komt u bij een website die dit zekerheidsniveau Midden vereist, dan wordt u gevraagd om naast uw DigiD gebruikersnaam en wachtwoord een eenmalige transactiecode in te toetsen. Die code ontvangt u dan binnen enkele seconden als sms bericht op uw mobiele telefoon.

Dit is een extra controle om uw identiteit vast te stellen. U bent immers de enige die precies op dat moment het sms'je met de specifieke transactiecode heeft ontvangen.

Voor de sms'jes die u ontvangt, hoeft u niet te betalen. Uw mobiele nummer wordt alleen gebruikt voor het toesturen van DigiD transactiecodes. Uw mobiele nummer zal nooit worden doorgegeven aan wie dan ook. Ook niet aan andere overheidsinstellingen.

4.10 Kennelijk zal dus gewerkt moeten worden met een gebruikersnaam, een wachtwoord en een sms-code. Dit roept wel veel praktische vragen op, zoals:

- Hoe doen we dat met verdachten/slachtoffers/getuigen die gedetineerd zitten?
- Hoe wordt omgegaan met personen die geen mobiele telefoon hebben?
- Hoe wordt omgegaan met personen die geen computer en/of internet hebben?
- Hoe wordt omgegaan met personen die in het buitenland wonen? Personen die niet over DigID beschikken?
- Hoe wordt omgegaan met rechtspersonen?
- Wat kan er worden gezegd over de koppeling van deze (zeer gevoelige!) informatie met andere overheidssystemen? Betekent dit dat ook de diverse overheidsinstanties (zoals de belastingdienst) inzage hebben in het strafdossier als geheel?

4.11 Los van deze nijpende zorgpunten vraagt de ACS zich af waarom de verdediging niet – net als het Openbaar Ministerie (zie p. 7, tweede alinea in het midden) – het procesdossier "gewoon" op een (beveiligde) USB-stick, cd-rom of dvd aangeleverd kan krijgen. In grote dossiers gebeurt dat in de praktijk ook al. De ACS verneemt graag waarom dit niet zou voldoen en wat de rechtvaardiging is voor het feit dat de verdediging (kennelijk) meer moeite moet doen om toegang tot stukken te krijgen dan het Openbaar Ministerie en de rechterlijke macht. Overigens wordt iets later in de besproken paragraaf 3.1 van de MvT wel nog opgemerkt dat elektronische documenten ook via een webportaal zou kunnen worden gedownload, dan wel beveiligd worden verzonden of via een gegevensdrager beschikbaar kunnen worden gesteld. De ACS stelt voor om deze laatste voorstellen als leidend te beschouwen, zodat de verdediging op dezelfde wijze kan kennisnemen van het digitale procesdossier. Dat voorkomt dat advocaten die op andere plekken dan op hun kantoor werkzaamheden verrichten, genoodzaakt worden al hun dossiergegevens 'in the cloud' te zetten. Tegen dat laatste bestaan bezwaren in verband met de beveiliging en de zekerheid van ononderbroken toegang tot die gegevens. Het is in ieder geval aangewezen hierover in de tekst van de MvT duidelijker te zijn.

4.12 Overigens beantwoorden deze laatste voorstellen (het webportaal, de beveiligde verzending of de verstrekking via een gegevensdrager) de bovengenoemde vragen niet (geheel). Een belangrijk probleem bij (uitsluitend) digitale verstrekking toegang blijft de wijze waarop gedetineerde daar toegang toe kunnen krijgen.

Vervangen van het papier dossier?

4.13 Dit brengt ons ook meteen op een ander belangrijk zorgpunt, namelijk de voorgenomen uiteindelijke vervanging van papieren processtukken door uitsluitend digitale processtukken. In de inleiding van de MvT (p. 8) wordt al opgemerkt dat de Archiefwet het mogelijk maakt dat *"papieren documenten elektronisch gereproduceerd en vervangen worden"*. De ACS vraagt zich bij lezing af of dit betekent dat die papieren documenten vervolgens ook *vernietigd* worden. Op p. 29 van de MvT lijkt hierop een antwoord te worden gegeven: vernietiging vindt plaats *"behoudens uitzonderingen"*. Uit de tekst blijkt niet aan welke uitzonderingen moet worden gedacht. De ACS raadt aan hierover meer duidelijkheid te geven.

4.14 In paragraaf 1.3.4 van de MvT wordt aangegeven dat sprake is van nevenschikking (p. 18). Er zal geen verplichting zijn voor justitiabelen of derden om langs elektronische weg stukken in te dienen of te kunnen ontvangen. Er is ook geen verplichting voor opsporingsinstanties, het

Openbaar Ministerie of de rechtspraak om alle handelingen met behulp van elektronische voorzieningen te doen en nog enkel elektronische stukken uit te wisselen (zie p. 18). De eerste alinea wordt vervolgens afgesloten met de volgende opmerking: *"Documenten in papieren of elektronische vorm kunnen naast elkaar worden gehanteerd."*

4.15 Dit roept in ieder geval de volgende vragen op:

- Op wiens verzoek kan er naast een elektronisch dossier ook nog een papieren dossier zijn (en andersom)? Kan ook de verdediging verzoeken om verstrekking van het papieren en/of het elektronisch dossier?
- Hoe moet deze opmerking worden gezien in verhouding tot de opmerking daarna dat digitale uitwisseling van het elektronisch strafdossier in 2016 de norm zal zijn?
- Bij wie rust de verantwoordelijkheid voor het ter beschikking stellen van een papieren dossier aan bijvoorbeeld de gedetineerde verdachte als alleen het elektronische dossier is verstrekt? Reeds nu wijst de ACS er op dat deze verantwoordelijkheid niet bij de advocatuur kan worden neergelegd. In de praktijk spreken we in grote zaken over vele orders met stukken. Wanneer deze uitsluitend digitaal beschikbaar worden gesteld, is het ondoenlijk om van de advocaat te verlangen om (zonder kostenvergoeding) voor zichzelf en voor zijn of haar cliënt het geheel te printen.

4.16 Een praktische oplossing voor in ieder geval een gedeelte van de opgeworpen vragen zou l kunnen worden gevonden in het stellen van een kwantitatieve grens. De ACS stelt voor dat , indien het procesdossier bijvoorbeeld meer dan 100 pagina's beslaat, aan de verdediging in ieder geval ook een papieren exemplaar ter beschikking wordt gesteld. Hiervan kan dan alleen worden afgeweken met uitdrukkelijke toestemming van de verdachte en/of diens advocaat.

Eisen aan de beveiliging na elektronische ontvangst

4.17 Opvallend is dat het wetsvoorstel alleen draait om de beveiliging van het elektronisch verkeer *tussen* de justitiabele en de rechterlijke macht, maar dat men zich kennelijk niet bekommert om de beveiliging van het elektronisch medium waarop de gegevens vervolgens worden ontvangen. Niet alleen het versturen van grote hoeveelheden data brengt echter risico's met zich mee, ook de opslag daarvan. We kennen allemaal de voorbeelden uit de media waarbij vertrouwelijke (justitiële) gegevens door de achterlating van een dossier in een trein of door het plaatsen daarvan aan de kant van de weg voor het grof vuil in handen van onbevoegde derden terecht kwamen. De oorzaak daarvan is veelal gelegen in onoplettendheid van degene die over dat dossier op dat moment de beschikking had. Gelet op de fysieke omvang van een dossier en de zorgvuldigheid waarmee daar in het algemeen mee wordt omgegaan, zijn dit uitzonderingen. Anders is het wanneer het gaat om een tablet of een andere gegevensdrager, zoals een USB-stick. Op die informatiedragers kunnen vele dossiers met een dito omvang aan vertrouwelijke gegevens van ontelbaar veel personen worden opgeslagen. Tablets zijn over het algemeen zeer gewilde objecten voor diefstal en USB-sticks zijn door hun geringe omvang makkelijk kwijt te raken. Het verliezen van een onbeveiligde stick met daarop zeer (privacy) gevoelige gegevens is onacceptabel. Daarbij wordt opgemerkt dat de meeste USB-sticks die in de winkel te koop worden aangeboden, geen standaardbeveiliging kennen.

4.18 De instantie (rechterlijke macht) die de gegevens verstrekt kan in dat verband niet denken 'na mij de zondvloed' en zijn ogen sluiten voor de risico's die het onbeveiligd opslaan van die gegevens met zich meebrengen. Een regeling als het onderhavige wetsvoorstel kan dan ook niet zonder de waarborg dat de gegevens beveiligd worden opgeslagen en dat daarmee zorgvuldig wordt omgegaan. Zij wordt dan ook, al dan niet middels een verwijzing naar een bij AMvB of richtlijn vast te leggen gedragscode voor alle procespartijen, in het wetsvoorstel node gemist. Voor zover de ontvangende partij een advocaat is, kan in dit verband worden gewezen op het Verenigd Koninkrijk, waar deze problematiek door middel van een in overleg met de

Orde van Advocaten aldaar opgestelde richtlijn is geregeld, te vinden onder de vermelding 'Guidelines on information security and government work' te vinden op: http://www.tsol.gov.uk/PanelCounsel/security.htm[1]

Elektronische aangifte en instellen van rechtsmiddelen

4.19 De informatieverstrekking *door* de verdachte, het slachtoffer en hun advocaten *aan* de overheid wordt behandeld in paragrafen 3.2- 3.5.

4.20 In paragraaf 3.2 van de MvT wordt voorgesteld het Besluit elektronische aangifte uit te breiden in die zin dat elektronische aangifte voor alle (!) strafbare feiten wordt geïntroduceerd. Elektronische aangifte kan alsdan op twee manieren plaatsvinden:

1. Mondelinge aangifte ten overstaan van een bevoegde ambtenaar. Deze ambtenaar stelt de aangifte elektronisch op en ook de ondertekening vindt elektronisch plaats. Er is dan geen papieren uitdraai meer.
2. Zelfstandige aangifte die langs elektronische weg aan de bevoegde ambtenaar ter beschikking wordt gesteld. De ambtenaar is dan niet betrokken bij het opstellen van de aangifte.

4.21 In de MvT wordt ten aanzien van de zelfstandige aangifte aangegeven dat ook deze zal dienen te geschieden met gebruikmaking van DigID (midden). De Minister signaleert hierbij (slechts) één probleem, namelijk de uitsluiting van personen (zoals toeristen) die niet beschikken over DigID. Maar omdat verwacht wordt dat deze personen zich voor aangifte sowieso wel bij het politiebureau zullen vervoegen, wordt dit probleem overruled door de voordelen bij het gebruik van DigID.

4.22 De Minister ziet over het hoofd dat er meer problemen zijn dan alleen toeristen zonder DigID. Want (ook hier): hoe zit het met gedetineerden die aangifte willen doen? Hoe zit het met advocaten die namens hun cliënten aangifte willen doen? Wiens DigID moeten zij daarvoor gebruiken? Het lijkt ons onwenselijk als de advocaat daarvoor gebruik zou moeten maken van zijn of haar persoonlijke DigID inloggevens. Overigens bestaat er momenteel al een praktijk van een aangiftebrief van de advocaat aan de (hoofd)officier van justitie. Eventueel kan worden gekozen voor het elektronisch versturen van deze aangiftebrief (bijvoorbeeld per e-mail), maar opgemerkt wordt dat de ACS het zeer wenselijk oordeelt dat deze praktijk blijft bestaan.

4.23 En voorts ook hier de zorg: hoe zit het met de koppeling van systemen? Met andere woorden: in hoeverre kan worden gegarandeerd dat de informatie uit de aangifte niet in ongewenste handen komt dan wel andere overheidsinstanties deze informatie zonder enig toezicht kunnen inzien en/of gebruiken? Deze informatie is immers niet getoetst. Het is dus zeker niet onwaarschijnlijk dat de informatie onwaarheden bevat.

4.24 Het is wat de ACS betreft aangewezen eerst op zijn minst deze vragen te beantwoorden en een zorgvuldige afweging te maken tussen de voor- en nadelen, voordat wordt gesteld dat in 2016 digitale aangifte de norm zal zijn. Een veilig, betrouwbaar en praktisch uitvoerbaar systeem is immers een onmisbare voorwaarde voor een dergelijk streven.

[1] snelkoppeling: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/263424/Guidelines_on_information_security_and_government_work_with_letter_from_AG_June_2010.pdf

Aanwenden van rechtsmiddelen

4.25 De ACS begrijpt dat het aanwenden en intrekken van rechtsmiddelen en het indienen van bezwaarschriften ook langs elektronische weg mogelijk zal worden (zie paragraaf 3.3.1 MvT). Ook de akte zal elektronisch worden opgemaakt. De griffier zal zijn elektronische handtekening zetten die voldoet aan de eisen van art. 138f Sv en de handtekening van de comparant zou volgens de MvT (weer) met gebruikmaking van DigID midden dienen te geschieden, dan wel met een "tablethandtekening" (zie voor tablethandtekening paragraaf 2.2.3 van de MvT).

4.26 Ten aanzien van gedetineerden geldt onder de huidige wetgeving een bijzondere regeling op grond van art. 451a Sv (kort gezegd de verstrekking van de schriftelijke verklaring van de gedetineerde aan het hoofd van de justitiële inrichting die dit vervolgens toezendt aan de griffie). Op p. 42 wordt in dit verband ten aanzien het volgende gesteld: *"Nu de gedetineerde binnen afzienbare termijn op de cel toegang kan hebben tot het internet zal nader worden bezien of aanpassing van deze bepaling is aangewezen, zodat de verklaring langs elektronische weg aan het hoofd van het gesticht kan worden overgedragen."* Vooruitlopend op deze mogelijke aanpassing, roept de ACS op een zeer zorgvuldige afweging te maken waarbij rekening wordt gehouden met het feit dat sommige gedetineerden helemaal niet binnen afzienbare tijd toegang hebben tot internet. Als voorbeelden noemen wij de preventief gedetineerden, met name in de eerste fase van de hechtenis, de preventief gedetineerden in alle beperkingen en de gedetineerden die in isolatie verblijven of anderszins beperkt zijn in hun vrijheden. Juist deze kwetsbare groep moet eenvoudig rechtsmiddelen kunnen instellen. Men bedenke daarbij dat de termijn van sommige rechtsmiddelen (zoals tegen de gevangenhouding) slechts drie dagen bedraagt.

Doen van verzet tegen strafbeschikking

4.27 Ook ten aanzien van het doen van verzet tegen de strafbeschikking wordt voorgesteld dit langs elektronische weg mogelijk te maken. Opvallend is dat in de MvT – anders dan bij gewone rechtsmiddelen – alleen de mogelijkheid via DigID wordt aangehaald (zie p. 43, eerste alinea laatste zin) en niet tevens een andere mogelijkheid zoals de tablethandtekening. Om redenen eerder genoemd (zie met name vragen onder 4.10) is het onwenselijk om dit onderscheid te laten bestaan en daarbij alleen het systeem van DigID van toepassing te laten zijn.

5. Conclusie

5.1 De ACS concludeert op grond van de voorafgaande beschouwingen dat het wetsvoorstel nog veel onduidelijkheden bevat. Samengevat gaat het om de volgende onderwerpen:

a) Er bestaat onduidelijkheid over de groep justitiabelen waarop deze nieuwe regels betrekking zullen hebben (4.8)
b) Er moet duidelijkheid komen over wat bedoeld wordt met de mogelijke verstrekking via "DigID midden" (4.9)
c) De mogelijkheid tot aanlevering van procesdossiers aan de verdediging op USB-stick, CD-Rom moet blijven bestaan (4.11)
d) Er moet duidelijkheid komen over de verkrijging van toegang tot digitale gegevens en de onbelemmerde mogelijkheid tot het doen van aangifte en aanwenden van rechtsmiddelen door gedetineerden (4.12, 4.20 en 4.23-4.25))
e) Er wordt melding gemaakt van de vernietiging van papieren dossiers 'behoudens uitzondering' terwijl ten onrechte niet duidelijk is om welke uitzonderingen het hier gaat (4.13-4.16)

f) Er is geen (verwijzing naar een) regeling met betrekking tot de beveiligde opslag van gegevens na ontvangst daarvan (4.17 – 4.18)
g) Niet duidelijk is waarom de wijze van instellen van een rechtsmiddel in geval van een strafbeschikking verschilt van andere situaties waarbij een rechtsmiddel wordt ingesteld (4.25).

Amsterdam, 6 januari 2014

Adviescommissie Strafrecht
mr. R. van der Hoeven, voorzitter,
namens deze, mr. R. Croes-Hoogendoorn, secretaris