ADVIES Nr 13 / 2006 van 24 mei 2006

O. Ref. : A / 2006 / 003

BETREFT : Identificatie en elektronische handtekening in de schoot van het informatiesysteem Phenix.

De Commissie voor de bescherming van de persoonlijke levenssfeer ;

Gelet op de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (hierna 'WVP'), inzonderheid artikel 29;

Gelet op het schrijven van de Voorzitter van het Hof van Cassatie van 18 januari 2006 en de adviesaanvraag vanwege de Minister van Justitie op 22 februari 2006 ;

Gelet op het verslag van de heer Peter Poma,

Brengt op 24 mei 2006 volgend advies uit:

1. VOORWERP VAN DE ADVIESAANVRAAG

1. Per brief van 22 februari 2006 heeft de Minister van Justitie de Commissie geraadpleegd aangaande de kwestie van de identificatie in de schoot van Phenix als algemene vraag over de verbanden tussen het informatiesysteem Phenix en het Rijksregister en meer in het bijzonder over de mogelijkheid om aan de uitvoerders van de rechtsbedeling (advocaten, gerechtsdeurwaarders, notarissen…) het gebruik van hun elektronische identiteitskaart op te leggen, zowel om toegang te verkrijgen tot Phenix als voor het elektronisch ondertekenen van elk document dat elektronisch wordt meegedeeld aan of neergelegd bij de griffie, alsook aangaande de wijze waarop de beroepslijsten van de uitvoerders van de rechtsbedeling zullen opgesteld worden.

2. Deze vraag vanwege de Minister van Justitie verleent gevolg aan een schrijven dat door de Voorzitter van het Hof van Cassatie gericht werd aan de Commissie waarin de identificatiemodaliteiten voor de advocaten in Phenix als volgt worden omschreven:

    1. Vervanging van het rijksregisternummer van de advocaten (meegedeeld naar aanleiding van het gebruik van hun elektronische identiteitskaart om toegang te verkrijgen tot Phenix) door een apart specifiek professioneel nummer.
    2. Verstrekking van een gerechtelijk elektronisch adres (e-mailadres) via de griffies.
    3. Gebruik van de elektronische handtekening wanneer een advocaat een elektronische proceduredaad stelt teneinde een garantie te verkrijgen aangaande authenticiteit en integriteit. (problematisch aangezien de ondertekeningsmodule van de elektronische identiteitskaart bij ieder gebruik naast de naam en de voornaam van de ondertekenaar ook diens rijksregisternummer meedeelt)

3. Het informatiesysteem Phenix werd ingevoerd door de wet van 10 augustus 2005 (hierna de wet Phenix 1). Het is eveneens aangewezen te verwijzen naar het wetsontwerp betreffende de elektronische procesvoering[1] dat momenteel besproken wordt in de kamercommissie Justitie (hierna het wetsontwerp Phenix 2). Deze beide bepalingen beogen een uniforme en gecentraliseerde informatisering van het gerechtelijk apparaat in België alsook de invoering van de elektronische procesvoering en dit zowel in burgerlijke als in strafzaken.

4. In toepassing van de vermelde wet van 10 augustus 2005 zijn de doeleinden van de verwerkingen en de verwerkingen die zullen plaatsvinden aan de hand van het systeem Phenix de volgende: de interne en externe communicatie vereist voor de werking van justitie, het beheer en de bewaring van gerechtelijke dossiers, de invoering van een nationale rol, de samenstelling van een databank met interne en externe rechtspraak, de opmaak van interne en externe statistieken alsook het verlenen van hulp bij het beheer en de administratie van de gerechtelijke instellingen. Deze doeleinden worden uitdrukkelijk geformuleerd in de artikelen 1 tot 14 van de bedoelde wet.

2. ALGEMENE BESCHOUWINGEN / FINALITEITS- EN WETTIGHEIDSBEGINSELEN VAN DE GEGEVENSVERWERKING

5. Uit **artikel 4, §1, ° van de WVP** blijkt dat persoonsgegevens **eerlijk en rechtmatig** dienen te worden verwerkt. Dit houdt in dat iedere verwerking van persoonsgegevens dient te gebeuren op een transparante wijze en met inachtneming van het recht. Bovendien vereist artikel 4, §1, 2° van de WVP dat de doeleinden van de verwerkingen **uitdrukkelijk omschreven en gerechtvaardigd** zijn.

6. **Wanneer een informatiesysteem verschillende doeleinden nastreeft,** dient de verantwoordelijke voor de verwerking te waken over **de transparantie van elke verwerking,** die hij met behulp van het systeem uitvoert, zodat de betrokkene zich bij de bewoordingen van

[1] Wetsontwerp betreffende de elektronische procesvoering, Parl.Doc; Kamer, 2004-2005, 51, 1701/001.

iedere finaliteit een redelijk beeld kan vormen over de aard van toepassingen die bedoeld worden met deze finaliteit en dit met het oog op het **controleren van de wettigheid** ervan.

7. Naast het belang van de wettelijke basis voor de verwerking van persoonsgegevens in de openbare sector, is het van belang dat de op die basis uitgevoerde verwerkingen overeenstemmen met het door de wet beoogde doeleinde en niet overmatig zijn ten opzichte hiervan. Het doeleinde van de verwerking mag niet leiden tot een overmatige schending van de belangen van de betrokkene namens de doeleinden die door de verantwoordelijke voor de verwerking worden beoogd.[2]

8. Wie zijn de **betrokkenen** waarvan de gegevens kunnen verwerkt worden dankzij het informatiesysteem Phenix? Het zijn zowel de te berechten personen als de uitvoerders van de rechtsbedeling en tenslotte de magistraten zelf.[3]

9. De Commissie heeft zich reeds uitgesproken over het informatiesysteem Phenix en verwijst naar het advies dat zij op 4 oktober 2004 (advies nr. 11/2004) heeft verstrekt over de twee voorontwerpen van wet tot oprichting van bedoeld informatiesysteem alsook naar het advies nr 41/1997 dat zij op eigen initiatief uitbracht op 23/12/1997 over de kwestie van de verspreiding van rechterlijke beslissingen.

10. De Commissie heeft in het advies nr. 11/2004 ondermeer opgemerkt dat het essentieel is dat een uniforme en gecentraliseerde informatisering van het gerechtelijk apparaat het **evenwicht tussen de belangen van de te berechten personen en het gerechtelijk apparaat** niet zou wijzigen en dat het hiertoe van belang is dat enerzijds **zekere beperkingen** zouden worden voorzien bij de verwerking van gerechtelijke gegevens en de toegang hiertoe en anderzijds een **transparantie** van de bij het gerechtelijk apparaat bestaande informatiesystemen de overhand zou hebben. Het is in het licht van die overwegingen dat de toegangsmodaliteiten en de werking van het informatiesysteem Phenix zullen moeten vastgelegd worden om niet alleen het recht op de bescherming van de persoonlijke levenssfeer van de betrokkenen te vrijwaren maar eveneens hun vertrouwen in de gerechtelijke diensten.

11. Het initiatief van de Minister en van de Voorzitter van het Hof van Cassatie om haar hierover opnieuw te raadplegen wordt dan ook gunstig onthaald door de Commissie. Het rekening houden met een dergelijk evenwicht is inderdaad belangrijk bij de beoordeling van de verbindingen tussen Phenix en andere databanken van de Staat zoals het Rijksregister.

2.1. Verbinding van Phenix met de andere databanken van de Staat

12. Wat de verbindingen betreft van het informatiesysteem Phenix met de andere databanken van de administratie zoals deze van het Rijksregister, voorziet **artikel 3 van de wet Phenix 1,** dat het doeleinde van de interne en externe communicatie van Phenix omschrijft, dat:

> «De interne communicatie heeft betrekking op de communicatie die is vereist voor de werking en het beheer van de hoven en rechtbanken en van de parketten ervan, alsmede voor het aanleggen en het beheren van de dossiers van de rechtspleging.

[2] Het Arbitragehof heeft zich trouwens onlangs uitgesproken over het proportionaliteitsbeginsel van de wet op de persoonlijke levenssfeer in het raam van het arrest nr 202/2004 van 21 december 2004 aangaande de wet van 6 januari 2003 betreffende de bijzondere opsporingsmethoden en enige andere onderzoeksmethoden in de volgende bewoordingen: Artikel 22 van de Grondwet houdt in dat “elke overheidsinmenging in het recht op eerbiediging van het privé-leven en het gezinsleven wordt voorgeschreven in een voldoende precieze wettelijke bepaling, beantwoordt aan een dwingende maatschappelijke behoefte en evenredig is met de daarin nagestreefde wettige doelstelling.” Het Hof heeft het noodzakelijk karakter van elke aangeklaagde bepaling geanalyseerd ten opzichte van de omschreven doelstellingen. Hieruit kan men enerzijds afleiden dat enkel de ernst van de opgespoorde feiten meer indringende onderzoeksmethoden rechtvaardigt en anderzijds het noodzakelijk karakter van het bestaan van een onafhankelijke en onpartijdige rechter om de wettigheid van de procedure te onderzoeken.

[3] Iedere toegang of daad die gesteld wordt binnen de elektronische ruimte van het justitiepaleis zal voortaan een spoor achterlaten op de servers van Phenix: aantal toegangen tot een dossier van een confrater, globaal aantal toegangen gedurende het jaar, weigering van elektronische betaling, controle van de werkzaamheden van een bepaalde magistraat….

De externe communicatie heeft betrekking op de kennisgeving, de betekening en de mededeling van de akten die zijn vereist in het kader van de gerechtelijke procedures, **alsmede op de communicatie met de openbare overheden om de nodige gegevens voor het samenstellen en het beheren van de gerechtelijke dossiers te verzamelen**»

13. De Commissie betreurt te moeten vaststellen dat, in tegenstelling tot de wens die zij uitdrukte in haar advies over de voorontwerpen van wet[4], deze finaliteit niet uitdrukkelijker wordt geformuleerd teneinde te beantwoorden aan de vereisten van het Europees hof voor de rechten van de mens inzake kwaliteit en duidelijkheid van de wet. Het gevaar op aantasting van het privéleven op dit punt werd reeds duidelijk gemaakt door de Commissie.

14. Vanaf het ogenblik dat wordt overwogen om het informatiesysteem Phenix te koppelen aan andere databanken van de administratie is het belangrijk dat de informatiestromen transparant zijn en dat de voorwaarden, modaliteiten en doeleinden van deze koppelingen verduidelijkt worden. Hiertoe raadt de Commissie het beheerscomité Phenix ten stelligste aan **verduidelijkingen aan te brengen wat betreft deze koppelingen** (welke databanken, voor welke doeleinden, onder welke voorwaarden en volgens welke modaliteiten?). Het beheerscomité is overeenkomstig artikel 17 van de wet Phenix 1 gemachtigd om terzake voorstellen te doen aan de Koning.

15. Het is inderdaad van belang dat een **controle** op deze koppelingen mogelijk wordt gemaakt, zowel in hoofde van de Commissie als van de betrokken personen. Een dergelijke controle is slechts mogelijk wanneer de verwerkingen openbaar en transparant zijn.

2.2. Het gebruik van het identificatienummer van het Rijksregister als identificatiemiddel voor de burger[5] waaromtrent in het informatiesysteem Phenix informatie wordt bewaard

16. Een doorgedreven studie over de persoonlijke identificatienummers werd in dit verband uitgevoerd door een **Comité van deskundigen inzake gegevensbescherming** onder de bescherming van het Comité européen de coopération juridique.[6] Deze studie maakt zowel gewag van de voordelen (duurzaamheid, administratieve vereenvoudiging, identificatie met grotere zekerheid dan wanneer enkel aan de hand van naam en voornaam) als de nadelen (gevaar op aantasting van de menselijke waardigheid door het reduceren van natuurlijke personen tot nummers, globale koppeling van de administratieve databanken, gevaar op uitsluiting van de betrokken persoon uit de informatiecircuits, gevaar op het volkomen verdwijnen van de anonimiteit van de burgers en hun recht op informatiezelfbeschikking) van het gebruik van een globaal uniek identificatiemiddel.

17. Tussen de conclusies van deze studie van de Raad van Europa bevinden zich de volgende principes:

    - « les PIN (Personal Identification Number) devraient **servir aux fins pour lesquelles ils sont créés et ne pas être utilisés à des fins non prévues au départ.** On pourrait par exemple douter du respect de ce principe si un PIN spécifique dont l'usage est strictement défini au départ sert à faciliter la comparaison de fichier, ou s'il est utilisé comme identifiant dans d'autre

[4] Advies nr. 11/2004, blz. 80 en 82

[5] Met "burger" wordt hier bedoeld de iedere natuurlijke persoon, andere dan een lid van de rechterlijke organisatie of een medewerker van het gerecht, waarover persoonsgegevens in het informatiesysteem Phenix worden verwerkt. Dit kunnen bijvoorbeeld zijn partijen in zaken van burgerlijk, handels- en sociaal recht (zoals eisers, verweerders, vrijwillig of gedwongen tussenkomende partijen, gedinghervattende partijen, …), verdachten, in beschuldiging gestelden, veroordeelden, burgerlijke partijen, getuigen, … De "burger" wordt daarbij onderscheiden van de leden van de gerechtelijke organisatie en van de medewerkers van het gerecht, zoals de advocaten, gerechtdeurwaarders of notarissen, die in het raam van hun functies hun persoonsgegevens beroepshalve in het informatiesysteem Phenix verwerkt zien.

[6] Beschikbaar op de website van de Raad van Europa op volgend adres: http://www.coe.int/T/F/Affaires_juridiques/Coop%E9ration_juridique/Protection_des_donn%E9es/Documents/Publications/4Pins.asp#TopOfPage

contextes (article 5.b de la Convention du 28/01/1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel);

- ❖ Le PIN devrait être **protégé contre l'accès illicite ou la diffusion à des tiers** (article 7 de la Convention) ;
- ❖ Le porteur du PIN devrait avoir le **droit d'accéder aux informations codées à l'aide du PIN,** de les faire rectifier et de les faire effacer, tout comme pour les fichiers de données à caractère personnel auxquels le PIN se rapporte (article 8 de la Convention) »

(vrije vertaling : officiële vertaling niet beschikbaar)

- ❖ « de PIN (Personal Identification Number) zouden **enkel moeten dienen voor de doelen waarvoor zij werden gecreëerd en niet gebruikt worden voor doeleinden waarvoor zij oorspronkelijk niet waren voorzien**. Men zou bijvoorbeeld de naleving van dit principe kunnen betwijfelen wanneer een specifieke PIN, waarvan het gebruik aanvankelijk strikt werd bepaald, gebruikt wordt om de vergelijking van een register te vergemakkelijken, of waneer hij als identificatiemiddel wordt gebruikt in andere contexten (artikel 5.b van het Verdrag van 28/01/1981 tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens);
- ❖ De PIN zou moeten **beschermd worden tegen ongeoorloofde toegang of verspreiding aan derden** (artikel 7 van het Verdrag) ;
- ❖ De houder van de PIN zou een **recht op toegang moeten krijgen tot de aan de hand van de PIN gecodeerde gegevens**, ze doen verbeteren of schrappen, zoals voor de registers met persoonsgegevens waarop de PIN betrekking heeft (artikel 8 van het Verdrag) »

18. Er dient eveneens te worden opgemerkt dat **het artikel 8 van de Richtlijn 95/45/EG**[7] handelt over de algemene identificatiemiddelen onder de afdeling **bijzondere categorieën van verwerkingen net zoals de gevoelige gegevens in de zin van de artikelen 6 tot 8 van de wet op de persoonlijke levenssfeer**. Overeenkomstig artikel 8.7 van de richtlijn stellen de Lidstaten de voorwaarden vast waaronder een nationaal identificatienummer of enig ander identificatiemiddel van algemene aard voor verwerkingsdoeleinden mag worden gebruikt.[8]

19. Het gebruik van het rijksregisternummer vertoont vanzelfsprekend **administratieve kwaliteiten** zoals de duurzaamheid, het unieke karakter, of het gebruiksgemak voor de veralgemeende koppelingen. Het gebruik van dit nummer als **uniek identificatiemiddel** vertoont **niet te verwaarlozen risico's** op aantasting van het recht op bescherming van het privéleven.

20. Een groot aantal Europese overheden inzake gegevensbescherming alsook bepaalde Europese regeringen hebben reeds principieel de verplichting opgelegd tot het gebruik van sectorale identificatiemiddelen (**Duitsland, Frankrijk, Portugal, Griekenland, Nederland, Italië, Oostenrijk**). Wat dit betreft heeft Oostenrijk zich nog recent op dit vlak onderscheiden voor zijn model van «citizen cards» privacy compliant in die zin dat enkel specifieke, per sector verschillende (fiscus, onderwijs, gezondheid…), identificatiemiddelen worden gebruikt en hun toekenning gebeurt door een onafhankelijke instantie.

21. De Commissie heeft reeds in haar vroegere adviezen[9] gesteld dat het aangewezen is om in **gevoelige domeinen specifieke sectorale identificatiemiddelen** te gebruiken.

[7] Richtlijn 95/46/EG van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens
[8] Cf. eveneens de consideransen 53 en 54 dienaangaande van de Richtlijn 95/46.
[9] Advies nr 01/2005 van 10 januari 2005, advies nr 10/2004 van 23 september 2004, advies nr 33/2002 van 22 augustus 2002, advies nr 30/2002 van 12 augustus 2002, advies nr19/2002 van 10 juni 2002, advies nr 14/2002 van 8 april 2002.

22. Naar aanleiding van haar advies over het voorontwerp van de wet Phenix (punt 25 van bedoeld advies) heeft de Commissie er overigens de nadruk op gelegd dat de codes en toegangssleutels tot de gerechtelijke dossiers geen direct verband mogen vertonen met de namen van de partijen, noch met die van hun vertegenwoordigers in rechte.

23. Reeds meerdere medewerkers van het gerecht zijn bij koninklijk besluit of, later, door het sectoraal comité van het Rijksregister gemachtigd om het identificatienummer van het Rijksregister te gebruiken. Dit is o.a. het geval in
   - artikel 591 van het Wetboek van Strafvordering dat voorziet dat de schriftelijk bij naam aangewezen ambtenaren van niveau 1 van de dienst van het Strafregister van het Ministerie van Justitie, alsook de hoofdgriffiers, de griffiers-hoofden van de griffie en de griffiers-hoofden van dienst van de hoven en rechtbanken van de rechterlijke orde, uitsluitend in het kader van het beheer van het Strafregister, toegang hebben tot de gegevens bedoeld in artikel 3, eerste lid, 1° tot 8°, en tweede lid, van de wet van 8 augustus 1983 tot regeling van een Rijksregister van natuurlijke personen en de identificatienummers van het Rijksregister van natuurlijke personen alleen mogen gebruiken voor de identificatie van de in het Strafregister opgenomen personen;
   - het koninklijk besluit van 30 september 1985 waarbij aan de onderzoeksrechters, aan de magistraten van het openbaar ministerie, aan de hoofdsecretarissen, aan de secretarissen-hoofden van dienst, aan de secretarissen, aan de adjunct-secretarissen en aan de opstellers die personeelslid zijn van de parketten, van de arbeidsauditoraten of van de krijgsauditoraten, toegang wordt verleend tot het Rijksregister van de natuurlijke personen en zij gemachtigd worden het identificatienummer van het Rijksregister van de natuurlijke personen aan te wenden (gewijzigd door door KB van 4 april 2003 en door het KB van 7 juli 2003);
   - het koninklijk besluit van 14 maart 1991 waarbij aan de griffiers van de hoven en rechtbanken van de Rechterlijke Orde toegang wordt verleend tot het Rijksregister van de natuurlijke personen en zij gemachtigd worden het identificatienummer van het Rijksregister van de natuurlijke personen aan te wenden;
   - het koninklijk besluit van 14 april 2002 waarbij de Koninklijke Federatie van het Belgisch Notariaat gemachtigd wordt om toegang te hebben tot de informatiegegevens van het Rijksregister van de natuurlijke personen en het identificatienummer ervan te gebruiken;
   - de beraadslaging RR Nr. 06 / 2006 van 01 maart 2006 betreffende de aanvraag van de Nationale Kamer van gerechtsdeurwaarders van België om in eigen naam en namens haar leden toegang te krijgen tot de informatiegegevens van het Rijksregister en om het identificatienummer van het Rijksregister te gebruiken met het oog op o.a. uitvoering van de artikelen 139 en 140 van de hypotheekwet.

24. Het is evenwel aangewezen om het onderscheid te maken tussen *een raadpleging* van het Rijksregister *met het oog op verificatie* van in bedoeld Register opgeslagen identificatiegegevens en *het gebruik* van het Rijksregisternummer als uniek identificatienummer voor personen. Het spreekt voor zich dat de verificatie van de in het Rijksregister opgeslagen gegevens door de medewerkers van Justitie, noodzakelijk is voor de uitoefening van de taken die onder hun bevoegdheid vallen, en het is dan ook om deze reden dat zij hiertoe werden gemachtigd. Zodoende kunnen de griffiers het Rijksregister van de natuurlijke personen raadplegen om bijvoorbeeld het huidige adres te kennen van een te berechten persoon om hem een procedureakte over te maken.

25. Het is eveneens van belang rekening te houden met artikel 7 van de wet Phenix 1 dat stelt dat **onverminderd de bepalingen van de wet van 8 augustus 1997 betreffende het Centraal Strafregister** « wordt in Phenix een interne gegevensbank voor de rechtspraak aangelegd teneinde de verschillende leden van eenzelfde gerecht de mogelijkheid te bieden de gerechtelijke dossiers te verwerken, alsmede een externe gegevensbank om de beslissingen

die belangrijk zijn voor de kennis en de ontwikkeling van het recht onder het publiek te verspreiden»[10]

26 Gelet op wat voorafgaat zou het **rijksregisternummer** niet op een *veralgemeende wijze* als identificatiemiddel van de te berechten personen mogen worden aangewend in de schoot van het informatiesysteem **Phenix,** vermits het gerechtelijk apparaat gegevens verwerkt die als gevoelig worden beschouwd (art.8 WVP) en dus een grotere bescherming vereisen inzake gegevensbescherming. Het is dus wenselijk dat zij in de schoot van het informatiesysteem Phenix worden geïdentificeerd aan de hand van een **specifiek nummer, verschillend van het rijksregisternummer**.

27. De Commissie dringt er op aan dat het gebruik van het identificatienummer van het Rijksregister in het kader van het informatiesysteem Phenix wordt omkaderd met een aantal waarborgen. Er moet immers worden vermeden dat het gebruik van het identificatienummer van het Rijksregister het al te eenvoudig mogelijk maakt om persoonsgegevens uit te wisselen of te koppelen op een wijze die niet in overeenstemming is met de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna 'Wet Verwerking Persoonsgegevens'), en in het bijzonder met het in artikel 4, §1, 3° van die wet neergelegde proportionaliteitsbeginsel. Het feit dat in het informatiesysteem Phenix voornamelijk gerechtelijke persoonsgegevens worden verwerkt, die krachtens artikel 8 van de Wet Verwerking Persoonsgegevens een bijzondere bescherming genieten, verhoogt de noodzaak om de nodige waarborgen te voorzien tegen onterechte uitwisselingen of koppelingen van persoonsgegevens

28. Daarenboven is de Commissie van oordeel dat, conform art 4, §1, 5° van de Wet Verwerking Persoonsgegevens,het identificatienummer van het Rijksregister niet meer in het informatiesysteem van Phenix mag worden opgeslagen indien het dossier wordt gearchiveerd en dus geen enkele gewettigde uitwisseling van persoonsgegevens meer nodig is. Op dat ogenblik dient het identificatienummer van het Rijksregister te worden verwijderd, zodat geen enkele mogelijkheid meer bestaat om actieve dossiers op basis van het identificatienummer van het Rijksregister met de gearchiveerde dossiers te koppelen.

29. Zoals reeds hoger aangegeven, is het, vanaf het ogenblik dat wordt overwogen om het informatiesysteem Phenix te koppelen aan andere databanken van de administratie, belangrijk dat de informatiestromen transparant zijn en dat de voorwaarden, modaliteiten en doeleinden van deze koppelingen verduidelijkt worden. Hiertoe raadt de Commissie het beheerscomité Phenix ten stelligste aan verduidelijkingen aan te brengen wat betreft deze koppelingen (welke databanken, voor welke doeleinden, onder welke voorwaarden en volgens welke modaliteiten?). Het beheerscomité is overeenkomstig artikel 17 van de wet Phenix 1 gemachtigd om terzake voorstellen te doen aan de Koning. Het is inderdaad van belang dat een controle op deze koppelingen mogelijk wordt gemaakt, zowel in hoofde van de Commissie als van de betrokken personen. Een dergelijke controle is slechts mogelijk wanneer de verwerkingen openbaar en transparant zijn.

30. Uiteraard is het gebruik van het identificatienummer van het Rijksregister niet toegelaten in de externe gegevensbank voor de rechtspraak noch bij de opmaak van statistieken. Volgens de artikelen 9, 10 en 12 van de wet van 10 augustus 2005 tot oprichting van het informatiesysteem Phenix dienen de gegevens voor deze doeleinden anoniem gemaakt te worden of gecodeerd te worden.

31. De Commissie stelt bijgevolg met genoegen vast dat op dit vlak technische maatregelen worden genomen om een dergelijk specifiek nummer te gebruiken en iedere veralgemeende

[10] Uit de debatten die hierover plaatshadden in de Senaatscommissie Justitie blijkt overigens dat de Minister van Justitie heeft verklaard dat de interne gegevensbank voor de rechtspraak in Phenix enkel dient om de magistraten van eenzelfde gerecht te helpen om eenheid in de rechtspraak aan te brengen en aldus aan een werkend magistraat de mogelijkheid te bieden alle vroeger door hem genomen beslissingen in gelijkaardige zaken terug te vinden en in voorkomend geval de motivering of het dispositief over te nemen (doc. Senaat nr. 3/1163/3)

opzoeking op basis van het rijksregisternummer van een natuurlijke persoon in de schoot van Phenix onmogelijk te maken. Wat dit betreft zouden de auteurs van het ontwerp zich desgevallend kunnen laten inspireren door de werkzaamheden die op dit niveau voor het project Bhealth (geïnformatiseerd medisch dossier) werden verricht door professor De Moor van de Gentse universiteit.[11].

32. Indien toch de weg van de codering van het rijksregisternummer van de natuurlijke personen door de auteurs van het project Phenix zou gekozen worden, is het noodzakelijk dat specifieke waarborgen worden voorzien opdat de ontcijferingssleutels enkel toegankelijk zouden zijn en gebruikt kunnen worden door de gemachtigde personen, mits naleving van de geldende wettelijke bepalingen en voor welbepaalde, precieze en transparante doeleinden en dit zowel voor de Commissie als voor de te berechten personen.

33. Kortom, het Rijksregisternummer mag in cijfertaal (gecodeerd) in het systeem Phenix opgeslagen worden maar mag geen identificatiesleutel zijn voor het systeem zelf. Het is dus aangewezen dat het gebruik van het rijksregisternummer in het systeem Phenix expliciet voorzien wordt in KB ter uitvoering van Phenix. Zo zal het aangewezen zijn om te verduidelijken welke personen zullen gemachtigd worden om houder te zijn van de ontcijferingsleutels en voor welke gerechtvaardigde, proportionele en transparante doeleinden een uitwisseling of koppeling van bestanden zal kunnen plaatsvinden op basis van dit nummer en mits inachtneming van de terzake geldende wettelijke bepalingen.

3. DE AUTHENTISERING VAN DE PERSONEN DIE TOEGANG HEBBEN TOT HET INFORMATIESYSTEEM PHENIX EN HET GEBRUIK VAN DE ELEKTRONISCHE IDENTITEITSKAART IN DAT VERBAND

34. Omwille van de bijzondere gevoeligheid van de gegevens verwerkt in het informatiesysteem Phenix, dient te toegang tot het systeem op een zeer goede wijze te worden beveiligd. In dat kader is het van wezenlijk belang dat de identiteit van elke gebruiker op een sluitende wijze kan worden geauthentiseerd en dat de hoedanigheid (bvb. rechter, griffier, advocaat, …) op basis waarvan een gebruiker toegang verwerft tot het systeem op een sluitende wijze kunnen worden geverifieerd. Onder authentisering wordt het proces verstaan waarbij wordt nagegaan of de identiteit die een gebruiker beweert te hebben om toegang te kunnen hebben tot het informatiesysteem Phenix, de juiste identiteit is. Authentisering van de identiteit kan geschieden op basis van een verificatie van kennis (vb. een paswoord), van een bezit (vb. een certificaat op een elektronisch leesbare kaart) maar de certificaten van de EID kaart zijn gebruiken op basis van een paswoord), van biometrische eigenschappen, of van een combinatie van meerdere van deze middelen. In casu lijkt een authentisering op basis van een gecombineerde verificatie van minstens kennis en bezit noodzakelijk. De aanvrager van een sessie zal dus in ieder geval moeten beschikken over een geheel van sleutels (userid, password en persoonlijke sleutel) De verificatie van de hoedanigheid is het proces waarbij wordt nagegaan of de hoedanigheid die een gebruiker beweert te hebben om toegang te hebben tot bepaalde onderdelen van het informatiesysteem Phenix, effectief een hoedanigheid is die deze gebruiker bezit. De verificatie van dergelijke hoedanigheid kan geschieden op basis van dezelfde soort middelen als deze gebruikt voor de authentisering van de identiteit van een gebruiker of, na authentisering van de identiteit van een gebruiker, door de raadpleging van een authentieke gegevensbank waarin de hoedanigheden m.b.t. de geïdentificeerde gebruiker worden opgeslagen of aan de hand van het gebruik van een elektronisch certificaat van beroepsauthentificatie.

35. Commissie is evenwel van oordeel dat alle middelen die kunnen worden gebruikt voor de authentisering van de identiteit evenals certificaten die zouden worden gebruikt voor het bewijs van een relevante hoedanigheid en zouden worden opgeslagen op een beroepskaart moeten voldoen aan de strenge eisen die zijn voorzien voor gekwalificeerde certificaten in de zin van de hoger vermelde wet van 9 juli 2001.

[11] Cf over dit onderwerp **http://www.health-telematics.be/behealth/20060120-bvt-gdm.pps**

36. Vooraleer aan een gebruiker de middelen worden ter beschikking gesteld waarmee hij zijn identiteit kan authentiseren en zijn hoedanigheid kan bewijzen, dient de betrokken identiteit en hoedanigheid uiteraard met een voldoende zekerheid te worden vastgesteld (door bijvoorbeeld een controle « face tot face» te organiseren.) Anders zou een gebruiker zich al te gemakkelijk een valse identiteit of hoedanigheid kunnen aanmeten. Het proces waarbij de identiteit en de hoedanigheden worden geregistreerd, moet dus sluitend zijn.

37. De Commissie stelt vast dat het certificaat dat ter authentisering van de identiteit is opgeslaan op de elektronische identiteitskaart voldoet aan de strenge eisen die voorzien zijn voor gekwalificeerde certificaten in de wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten. De vereisten voor gekwalificeerde certificaten betreffende het certificaat zelf (bijlage I van de wet) alsook de certificatiedienstverlener (bijlage II) die ze aflevert én de vereisten voor het veilig middel voor het aanmaken van een handtekening (bijlage III) werden gerespecteerd voor de certificaten voor authentisering, slechts met uitzondering van de elementen die onlosmakelijk verbonden zijn met het handtekenen en niet kunnen worden toegepast voor authentisering.

38. De Commissie is van oordeel dat de in de elektronische identiteitskaart aanwezige authentificatiecertificaat voldoende waarborgen biedt voor de authentificatie van de identiteit van een gebruiker van het informatiesysteem Phenix. Aangezien dit certificaat evenwel geen bewijs van hoedanigheid inhoudt, kan deze laatste gecontroleerd worden aan de hand van een authentieke gegevensbank waarin de relevante hoedanigheid wordt opgeslagen en beheerd in samenwerking met de authentieke bronnen van deze hoedanigheden die gevormd worden door de verschillende betrokken beroepsorden indien deze bestaan. In deze gegevensbanken zullen de rijksregisternummers van de leden kunnen opgenomen worden zodat een verband kan gelegd worden tussen bedoeld nummer en de hoedanigheid van de titularis.

39. Wat de opportuniteit betreft om het gebruik van de elektronische identiteitskaart al dan niet op te leggen en hoewel het onderscheid dient gemaakt te worden tussen de traditionele functie van de identiteitskaart, zijnde identificatie (voorlegging) en haar twee nieuwe functies, zijnde de elektronische authentificatie[12] en elektronische handtekening[13][14], merkt de Commissie dienaangaande op dat **in toepassing van artikel 6, §7[15] van de voormelde wet van 19 juli 1991 de Koning , na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, naast de autoriteiten en openbare overheden waaraan de identiteitskaart op hun vraag moet worden voorgelegd[16], eveneens de gebruiksmodaliteiten van de identiteitskaart bepaalt.**

40. Een onvoorwaardelijke en niet gerechtvaardigde veralgemening van dit gebruik zou strijdig zijn met de finaliteits-, proportionaliteits-en wettigheidsbeginselen van de wet op de persoonlijke

[12] Actief proces waarbij de houder van een elektronische identiteitskaart zich vrijwillig en elektronisch identificeert. Dit wordt bevestigd door het elektronisch certificaat afgeleverd door Certipost in zijn hoedanigheid van betrouwbare derde die belast is met de opdracht tot het afleveren en het beheer van de certificaten voor authentificatie en elektronische handtekening van de identiteitskaart.

[13] Het technisch proces van de elektronische handtekening is identiek aan dit van de elektronische authentificatie met dit verschil dat in het proces van elektronische handtekening gaat om een semantische boodschap die gecodeerd wordt terwijl het in het authentificatieproces gaat om een door de kaart gecreëerd willekeurig getal dat gecodeerd wordt.

[14] Het Verslag aan de Koning, voorafgaand aan het KB van 25 maart 2003 maakt eveneens het onderscheid tussen de verschillende functies van de elektronische identiteitskaart. Men kan hier lezen dat ingeval van gebruik van de elektronische identiteitskaart op afstand, enkel het aspect authentificatie en elektronische handtekening bruikbaar is en dat de verschillende identiteitsgegevens noch met het blote oog, noch elektronisch leesbaar zijn. Bovendien lijkt het Verslag aan de Koning zich te baseren op de noodzaak van **toestemming** door de houder voor het elektronisch ontvangen van de identiteitsgegevens voorzien bij artikel 6 van de wet van 19 juli 1991.

[15] Art.6 §7 Wet 19/07/1991" De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, ingesteld bij de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, de vorm en de modaliteiten van aanmaak, afgifte **en gebruik** van de identiteitskaart."

[16] Zoals voorzien in artikel 1 van het KB van 25/03/2003 betreffende de identiteitskaarten.

levenssfeer, alsook met het Verslag aan de Koning voorafgaand aan het KB van 25 maart 2003.

41. Wat dit betreft zou het eveneens aangewezen zijn dat de wetgever zich vragen stelt over de **risico's die gepaard gaan met de creatie** van een **uitbreiding van het gebruik van de identiteitskaart tot alle activiteiten van een individu** terwijl de identiteitskaart zich tot op heden enkel beperkte tot de intieme sfeer van een individu en niet tot zijn werkkring.

42. Bovendien, niet alle gebruikers van het informatiesysteem Phenix beschikken echter over een elektronische identiteitskaart. Men denke bijvoorbeeld aan buitenlandse advocaten. Daarenboven staat het elke titularis van een elektronische identiteitskaart vrij om, conform artikel 6, § 2, laatste lid van de wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, de certificaten op zijn kaart niet te activeren. Overigens is de Commissie van oordeel dat het niet wenselijk is dat een gebruiker van het informatiesysteem Phenix zou worden verplicht om zijn elektronische identiteitskaart te gebruiken voor de authentisering van zijn identiteit ten aanzien van het informatiesysteem Phenix.

43. Tenslotte blijkt uit artikel 6, § 2 van de wet van 19 juli 1991 dat de keuze om een beroep te doen op een geaccrediteerde certificatiedienstverlener voor de elektronische identiteitskaart gemaakt werd door de wetgever[17]. Welnu, tot op heden blijkt geen enkele geaccrediteerde certificatiedienstverlener een accreditatie te hebben verkregen. Volgens de Europese Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen en de wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten is de accreditatie van de certificatiedienstverlener geen voorwaarde voor de geldigheid van de handtekeningen. Een geavanceerde handtekening, gecreëerd met een veilig middel voor het aanmaken van een handtekening, gebaseerd op een gekwalificeerd certificaat dat is afgeleverd door een certificatiedienstverlener die voldoet aan de voorwaarden van bijlage II van de wet, is een geldige handtekening met dezelfde effecten als een handgeschreven handtekening. Nochtans vermeldt men in de wet van 19 juli 1991 betreffende de bevolkingsregisters en de identiteitskaarten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, dat het in het geval van de certificaten op de elektronische identiteitskaart, gaat om een geaccrediteerde certificatiedienstverlener. Hoewel de accreditatie strikt genomen geen invloed heeft op de geldigheid van de handtekening, is de Commissie van oordeel dat de wet gerespecteerd dient te worden.

4. Samenstelling van beroepslijsten

44. De Minister van Justitie raadpleegt de Commissie eveneens over de wijze waarop de beroepslijsten van de actoren van Phenix kunnen gecreëerd worden.

45. Teneinde een sterke authentificatie (beschreven onder punt 40) van de actoren in de schoot van Phenix mogelijk te maken, voorziet het wetsontwerp betreffende de elektronische procesvoering in zijn artikelen 23 tot 25 en 53 de opmaak van **beroepslijsten** die **openbaar** zullen zijn.

46. Overeenkomstig artikel 4 van de wet op de persoonlijke levenssfeer is het belangrijk dat deze lijsten enkel gegevens bevatten die terzake dienend zijn en niet overmatig voor de realisatie van het doeleinde dat erin bestaat zich te verzekeren over de hoedanigheid van een uitvoerder van de rechtsbedeling. Wanneer het enkel de bedoeling is de functie van een

[17] Artikel 17 van de wet van 9/07/2001 voorziet inderdaad een procedure van vrijwillige accreditatie voor de geaccrediteerde certificatiedienstverleners waardoor aan deze dienstverleners als het ware een kwaliteitslabel wordt toegekend na controle door de administratie. Dit kwaliteitslabel zou aldus de conformiteit van de dienstverlener met de voorwaarden van de bijlagen van de wet bevestigen en dus ondermeer inzake gegevens inbegrepen in het certificaat.

persoon te identificeren, volstaat het dat in de lijst enkel de daartoe naadzakelijke gegevens worden opgenomen, zijnde **de naam, de voorna(a)m(en), de hoedanigheid van de uitvoerder van de rechtsbedeling alsook zijn beroepsadres(sen) en in voorkomend geval zijn gerechtelijk elektronisch adres.** Andere, niet ter zake dienende gegevens, moeten bijgevolg het voorwerp te uitmaken van een toestemming van de betrokkene.

5. IDENTIFICATIE VAN DE LEDEN VAN DE GERECHTELIJKE ORGANISATIE EN VAN DE MEDEWERKERS VAN HET GERECHT BINNEN HET INFORMATIESYSTEEM ZELF VOOR ANDERE DOELEINDEN DAN DE TOEGANGSCONTROLE EN HET AANMAKEN VAN LOGGINGS

47. Volgens de inlichtingen die de Commissie heeft verkregen over de huidige stand van zaken aangaande de architectuur van het informatiesysteem, zullen de leden van de gerechtelijke organisatie, de advocaten en de uitvoerders van de rechtsbedeling, eenmaal zij de toegangscontrole (zoals hierboven beschreven) voorbij zijn, en met uitzondering van de identificatie via de door de betrokken beroepsorganisatie gekozen loggins, geïdentificeerd worden binnen het informatiesysteem zelf, naar keuze, hetzij aan de hand van het identificatienummer van het Rijksregister, hetzij aan de hand van een specifiek identificatienummer. Zo zou er een **specifiek identificatienummer** gebruikt kunnen worden voor de advocaten (**uniek advocatennummer** dat de plaats inneemt van het rijksregisternummer van de advocaat), of voor de leden van de rechterlijke orde (het inschrijvingsnummer voor de magistraten, griffiers,…).

48. Gelet op de hierboven geformuleerde overwegingen van de Commissie, is de Commissie van oordeel dat het gebruik binnen Phenix van een dergelijk sectoraal identificatiemiddel voor bepaalde beroepsgroepen een nuttig middel is voor de toepassing van het proportionaliteitsbeginsel vervat in artikel 4 van de Wet Verwerking Persoonsgegevens op de identificatiemiddelen, voorzover dit technisch mogelijk is en in niets het veiligheidsniveau van Phenix aantast.

6. GEBRUIK VAN DE ELEKTRONISCHE HANDTEKENING BINNEN HET INFORMATIESYSTEEM PHENIX EN HET GEBRUIK VAN DE ELEKTRONISCHE IDENTITEITSKAART IN DAT VERBAND

49. De wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten bepaalt de voorwaarden waaronder een elektronische handtekening automatisch dezelfde juridische gevolgen heeft als een handgeschreven handtekening.

50. Artikel 4, § 4 van de wet bepaalt dat een geavanceerde elektronische handtekening gerealiseerd op basis van een gekwalificeerd certificaat en gemaakt door middel van een veilig middel voor het aanmaken van een handtekening, geassimileerd wordt met een handgeschreven handtekening. Dergelijke elektronische handtekening wordt een gekwalificeerde elektronische handtekening genoemd en wordt als voldoende veilig beschouwd om automatisch gelijkgesteld te worden met een handgeschreven handtekening zonder dat de rechter hierbij zal moeten nagaan of de nodige veiligheidsgaranties aanwezig zijn.

51. Een gekwalificeerd certificaat is volgens de wet een certificaat dat voldoet aan de eisen van bijlage I van deze wet en dat wordt afgegeven door een certificatiedienstverlener die voldoet aan de eisen van bijlage II van dezelfde wet. De certificatiedienstverlener voor de certificaten van de elektronische identiteitskaart Certipost, heeft overeenkomstig artikel 4 § 2 van de voormelde wet van 9 juli 2001, bij de FOD Mineco aangifte gedaan van de aflevering van gekwalificeerde certificaten. De lijst van certificatiedienstverleners die dergelijke certificaten afleveren is gepubliceerd op de website van de FOD Mineco.

52. Het **artikel 5**[18] bepaalt dat elke certificatiedienstverlener die voor het publiek bestemde certificaten afgeeft enkel **rechtstreeks** bij de betrokken persoon **of met diens uitdrukkelijke toestemming persoonlijke gegevens mag inwinnen en enkel indien dit noodzakelijk is voor de afgifte en de bewaring van het certificaat**.

53. Daarenboven beschrijft **bijlage 1** van de wet "elektronische handtekening" de gegevens die elk gekwalificeerd certificaat moet bevatten. Onder deze gegevens bevindt zich de mogelijkheid om desgevallend een **specifieke kwalificatie** van de ondertekenaar bij te voegen in functie van de gebruiksbestemming van het certificaat.

54. Als een veilig middel voor het aanmaken van een handtekening wordt volgens de wet beschouwd geconfigureerde hard- en software die wordt gebruikt om de gegevens voor het aanmaken van een handtekening te implementeren en die voldoet aan de eisen van bijlage III van de wet. De processorchipkaart die de drager is van de elektronische identiteitskaart, voldoet hieraan.

55. De geavanceerde elektronische handtekening is in artikel 2, 2° als volgt gedefinieerd:
"Elektronische gegevens vastgehecht aan of logisch geassocieerd met andere elektronische gegevens, die worden gebruikt als middel voor authentificatie en aan de volgende eisen voldoet:
    a) zij is op unieke wijze aan de ondertekenaar verbonden;
    b) zij maakt het mogelijk de ondertekenaar te identificeren;
    c) zij wordt aangemaakt met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
    d) zij is op zodanige wijze aan de gegevens waarop zij betrekking heeft verbonden, dat elke latere wijziging van de gegevens kan worden opgespoord."

56. De Commissie stipt aan dat de implementatie van de certificaten voor elektronische handtekening van de elektronische identiteitskaart, zo is opgevat **dat aan de bestemmeling van een elektronisch, door middel van de elektronische identiteitskaart ondertekend document automatisch de naam, de eerste twee voornamen en het rijksregisternummer van de houder van de kaart worden meegedeeld**.[19] (vermits het rijksregisternummer wordt gebruikt als serienummer voor de certificaten van de elektronische identiteitskaart)

57. **De Commissie stelt zich vragen over dit punt en zou de bestaansreden willen vernemen van deze systematische mededeling van het rijksregisternummer, bovenop deze van de naam en de eerste twee voornamen.**

[18] Art. 5. § 1. Onverminderd de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten aanzien van de verwerking van persoonsgegevens, mag een certificatiedienstverlener die voor het publiek bestemde certificaten afgeeft enkel rechtstreeks bij de betrokken persoon of met diens uitdrukkelijke toestemming persoonlijke gegevens inwinnen en enkel indien dit noodzakelijk is voor de afgifte en de bewaring van het certificaat. De gegevens mogen niet voor andere doeleinden worden verzameld of verwerkt zonder de uitdrukkelijke toestemming van de betrokken persoon.
§ 2. Wanneer de houder van het certificaat een pseudoniem gebruikt en wanneer het onderzoek dit vereist, is de certificatiedienstverlener die het certificaat heeft afgegeven ertoe gehouden alle gegevens betreffende de identiteit van de titularis mee te delen in de omstandigheden en volgens de voorwaarden waarin de artikelen 90ter tot 90decies van het Wetboek van Strafvordering voorzien.

[19] Newsletter nr 1 over de elektronische identiteitskaart, beschikbaar op de website van de Minister van Binnenlandse Zaken (Rijksregister)

58. De Commissie wijst er evenwel op dat het verder gebruik van het identificatienummer van het Rijksregister door de bestemmeling van het handtekeningcertificaat, behoudens in de gevallen bepaald door de Koning bij in Ministerraad overlegd besluit na advies van het sectoraal comité van het Rijksregister, onderworpen is aan een machtiging van het sectoraal comité van het Rijksregister. Het identificatienummer van het Rijksregister vervat in het handtekeningcertificaat opgeslagen op de elektronische identiteitskaart mag in de huidige stand van de regelgeving aldus enkel verder verwerkt worden door instanties die hiertoe gemachtigd zijn Instanties die niet over een dergelijke machtiging beschikken en ten aanzien waarvan een elektronische handtekening wordt geplaatst op basis van de elektronische identiteitskaart mogen het identificatienummer van het Rijksregister niet verder verwerken. Technisch moet ervoor gezorgd worden dat het certificaat in die gevallen slechts gebruikt wordt voor de validatie van de elektronische handtekening met uitsluiting van elke verdere verwerking. Met het oog op bewijsvoering moet, conform artikel 4, §1, 3° van de Wet Verwerking Persoonsgegevens, slechts bewaard worden wat als toereikend, terzake dienend en niet overmatig beschouwd kan worden.

59. Artikel 4, § 3 van de wet van 9 juli 2001 stelt dat de Koning bij een besluit vastgesteld na overleg in Ministerraad, voor het gebruik van elektronische handtekeningen in de openbare sector eventuele aanvullende eisen kan stellen. Deze eisen moeten objectief, transparant, evenredig en niet discriminerend zijn en slechts op de specifieke kenmerken van de betrokken toepassing betrekking mogen hebben. Zij mogen geen belemmering vormen voor grensoverschrijdende diensten. Zonder afbreuk te doen aan de bedenkingen van de Commissie over de huidige configuratie van de certificaten kan dit artikel de grondslag vormen voor een regeling waarbij voor het gebruik van de elektronische handtekening in het kader van informatiesysteem Phenix de veiligheidsvereisten voor de handtekening worden opgelegd.

60. Uit de artikelen 7 en 23 van het wetsontwerp Phenix 2 vloeit voort dat de enige verplichting inzake elektronische handtekening die wordt opgelegd aan de toekomstige gebruikers van Phenix het gebruik is van de gekwalificeerde elektronische handtekening. De keuze lijkt gerechtvaardigd omdat een dergelijke elektronische handtekening als enige geniet van het principe van automatische assimilatie met de handgeschreven handtekening omwille van de eraan geassocieerde veiligheidsgaranties. Een elektronische handtekening geplaatst aan de hand van de elektronische identiteitskaart is een gekwalificeerde elektronische handtekening. Ook gekwalificeerde elektronische handtekeningen geplaatst aan de hand van andere middelen dan de elektronische identiteitskaart moeten echter mogelijk zijn.

61. De Commissie meent dat **het gebruik van een professioneel handtekeningcertificaat zou kunnen overwogen worden** in die mate dat deze oplossing het voordeel biedt, enerzijds, het beoogde doeleinde te bereiken dat erin bestaat elektronisch te ondertekenen en hierbij zijn specifieke hoedanigheid te bewijzen zonder dat het rijksregisternummer wordt gebruikt en anderzijds, een uitbreiding van het gebruik van de elektronische identiteitskaart tot de beroepssfeer te vermijden. Dergelijke certificaten zouden inderdaad de specifieke professionele hoedanigheid van de ondertekenaar kunnen bewijzen.

62. Deze certificaten zouden kunnen beheerd worden door een **betrouwbare derde** in samenwerking met de betrokken beroepsorganisaties. Deze betrouwbare derde zou desgevallend de communicatiedienstverlener[20] kunnen zijn wiens activiteiten geregeld zijn in het wetsontwerp Phenix 2 voor zover dat uit artikel 10, §1, 2° volgt dat deze “aan de hand van de gepaste en wettelijke middelen de identiteit van de partijen bij de betekening, de kennisgeving of de mededeling nagaan”.

[20] Artikel 2, 4° van het wetsontwerp Phenix 2 beschrijft deze dienstverleners als volgt : “onderneming die beantwoordt aan de voorwaarden vastgelegd in artikel 10 van deze wet, alsook aan die bepaald door de Koning, na advies van het beheerscomité en van het toezichtcomité, en die optreedt als intermediair orgaan bij elke betekening, kennisgeving, neerlegging of mededeling in het kader van een gerechtelijke procedure”.

OM DEZE REDENEN,

Brengt de Commissie een gunstig advies uit voor zover er technische maatregelen worden genomen opdat een sectoraal identificatienummer, verschillend van het rijksregisternummer (cfr supra punt 33) zou gebruikt worden voor de te berechten personen om, ondermeer, iedere opzoeking op basis van het rijksregisternummer te vermijden.

In antwoord op de vragen die haar werden gesteld, beveelt de Commissie aan :

- dat er maatregelen worden genomen met het oog op het gebruik van de professionele elektronische certificaten die de in punt 59 beschreven voordelen bieden;
- de tussenkomst van de wetgever om de gebruiksmodaliteiten van de identiteitskaart te preciseren;
- dat de openbare beroepslijsten enkel zouden bestaan uit terzake dienende gegevens, de andere zouden moeten gewettigd worden via de toestemming van de betrokken personen.

De administrateur, De voorzitter,

(get.) Jo BARET (get.) Michel PARISSE