AVIS N° 13 / 2006 du 24 mai 2006

N. Réf. : SA2 / A / 2006 / 003

OBJET : Identification et signature électronique au sein du système d'information Phenix.

La Commission de la protection de la vie privée,

Vu la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel (ci-après, « LVP »), en particulier, l'article 29 ;

Vu le courrier du Président de la Cour de la Cassation du 18 janvier 2006 et la demande d'avis de la Ministre de la Justice du 22 février 2006;

Vu le rapport de Monsieur Peter Poma,

Emet le 24 mai 2006, l'avis suivant :

1. OBJET DE LA DEMANDE D'AVIS

1. Par courrier du 22 février 2006, la Ministre de la Justice a interrogé la Commission sur les question d'identification au sein de phenix en tant que question générale des liens du système d'information Phenix avec le Registre National et plus précisément notamment sur la possibilité d'imposer aux auxiliaires de justice (avocats, huissiers, notaires …) d'utiliser leur carte d'identité électronique tant pour accéder à Phenix que pour signer électroniquement tout document communiqué et déposé de façon électronique aux greffes, et sur la façon dont les listes professionnelles des auxiliaires de justice seront créées.

2. Cette demande de la Ministre de la Justice fait suite à un courrier du Président de la Cour de Cassation adressé à la Commission dans lequel sont décrites les modalités d'identification des avocats au sein de Phenix de la manière suivante :

    1. Substitution du numéro de registre national des avocats (communiqué lors de l'utilisation de leur carte d'identité pour accéder à Phenix) par un numéro professionnel spécifique distinct
    2. Délivrance d'une adresse judiciaire électronique (adresse email) via les greffes
    3. Utilisation de la signature électronique lorsqu'un avocat procède à un acte de procédure par voie électronique afin d'obtenir toute garantie d'authenticité et d'intégrité. (problématique étant donné que module de signature électronique de la carte d'identité électronique communique lors de chaque utilisation en plus du nom et du prénom du signataire son numéro de registre national)

3. Le système d'information Phenix a été institué par la loi du 10 août 2005 (ci-après la loi Phenix 1). Il convient également de se référer au projet de loi relatif à la procédure par voie électronique[1] en cours de discussion en Commission Justice de la Chambre (ci-après le projet de loi Phenix 2). Ces deux dispositions ont pour objectif l'informatisation uniforme et centralisée de l'appareil judiciaire en Belgique ainsi que l'introduction de la procédure par voie électronique tant en matière civile qu'en matière pénale.

4. En vertu de ladite loi du 10 août 2005, les finalités des traitements et opérations de traitements qui seront opérés à l'aide du système d'information Phenix sont les suivantes : la communication interne et externe requise par le fonctionnement de la justice, la gestion et la conservation des dossiers judiciaires, l'instauration d'un rôle national, la constitution d'une banque de données de jurisprudence interne et externe, l'élaboration de statistiques internes et externes ainsi que l'aide à la gestion et à l'administration des institutions judiciaires. Ces finalités sont explicitées aux articles 1 à 14 de ladite loi.

2. CONSIDERATIONS GENERALES / PRINCIPES DE FINALITE ET DE LEGITIMITE DES TRAITEMENTS DE DONNÉES

5. Il ressort de **l'article 4, §1, 1° de la LVP** que tout traitement de données à caractère personnel doit être **loyal et licite**. Cela implique que tout traitement de données doit ainsi avoir lieu de façon transparente et dans le respect du droit. En outre, l'article 4, §1, 2° de la LVP exige que les **finalités** des traitements de données à caractère personnel soient **déterminées, explicites et légitimes**.

6. **Si un système d'information poursuit diverses finalités**, il appartient au responsable de traitement de veiller à la **transparence de chacun des traitements** qu'il opère à l'aide dudit système de manière à ce que la personne concernée puisse raisonnablement, à l'énoncé de chaque finalité, concevoir les types d'application couverts par cette finalité, ceci afin de permettre le **contrôle de légitimité**.

[1] Projet de loi relatif à la procédure par voie électronique, *Doc. Parl*., *Ch*., 2004-2005, 51, 1701/001.

7. Outre l'importance de la base légale des traitements de données dans le secteur public, il importe que les traitements effectués sur cette base soient conformes au but poursuivi par la loi et non disproportionnés à celui-ci. La finalité du traitement ne peut en effet induire une atteinte disproportionnée aux intérêts de la personne concernée au nom des intérêts poursuivis le responsable de traitement**.** [2]

8. Qui sont **les personnes concernées** à propos desquels des traitements pourront être opérés grâce au système d'information Phenix? Ce sont à la fois les justiciables, les auxiliaires de justices, les avocats et enfin les magistrats eux-mêmes[3].

9. La Commission s'est déjà prononcée sur le système d'information Phenix et renvoie aux avis qu'elle a émis sur les deux avant-projets de loi instituant ledit système d'information le 4 octobre 2004 (avis n°11/2004) ainsi que sur la question de la diffusion des décisions juridictionnelles dans son avis n°41/1997 émis d'initiative le 23/12/1997.

10. La Commission a notamment relevé dans cet avis n°11/2004 qu'il est fondamental que l'informatisation centralisée et uniforme de l'appareil judiciaire ne modifie pas **l'équilibre des intérêts entre le justiciable et l'appareil judiciaire** et qu'à ce titre, il importe que d'une part soient fixées **certaines limites** dans le traitement des données judiciaires et leurs accès et que d'autre part prévale une **transparence** des flux d'informations au sein de l'appareil judiciaire. C'est au regard de ces considérations que les règles d'accès et de fonctionnement du système d'information Phenix devront être définies pour préserver non seulement le droit à la vie privée des personnes concernées mais également leur confiance dans les services de la Justice.

11. . La Commission accueille dès lors favorablement l'initiative de la Ministre de la Justice et du Président de la Cour de Cassation de la consulter à nouveau. La prise en compte d'un tel équilibre est effectivement importante dans l'appréciation des liens entre Phenix et les autres bases de données de l'Etat telles que le registre national.

2.1 Liaison de Phenix aux autres bases de données de l'Etat.

12. Concernant les liens entre le système d'information Phenix et les autres bases de données de l'administration telles que celle du Registre national, **l'article 3 de la loi Phenix 1** décrivant la finalité de communication externe et interne de Phenix prévoit que

> « La communication interne vise les communications requises pour le fonctionnement et la gestion des cours et tribunaux et de leurs parquets, ainsi que par la constitution et la gestion des dossiers de procédure.
> La communication externe vise la notification, la signification et la communication des actes requis par les procédures judiciaires, **ainsi que la communication avec les autorités publiques destinée à la collecte des données nécessaires pour l'élaboration et la gestion des dossiers judiciaires** »

[2] La Cour d'Arbitrage s'est d'ailleurs récemment prononcée sur le principe de proportionnalité de la loi vie privée dans le cadre de l'arrêt n°202/2004 du 21 décembre 2004 à propos de la loi du 6 janvier 2003 concernant les méthodes particulières de recherche et quelques autres méthodes d'enquête en ces termes: L'article 22 de la Constitution implique que "toute ingérence des autorités dans le droit au respect de la vie privée et familiale soit prescrite par une disposition législative suffisamment précise, corresponde à un besoin social impérieux et soit proportionnée à l'objectif légitime poursuivi par celle-ci." La Cour a analysé le caractère nécessaire de chaque disposition incriminée au regard des objectifs décrits. L'on peut en déduire d'une part que seule la gravité des infractions recherchées justifie l'utilisation de méthodes de recherche plus invasives et d'autre part le caractère nécessaire de l'existence d'un juge indépendant et impartial pour effectuer la légalité des procédures.

[3] Toute entrée ou acte désormais posé dans l'enceinte électronique du Palais de Justice laissera désormais des traces dans les serveurs de Phenix : nombre d'accès au dossier d'un confère, nombre d'accès globaux sur l'année, refus de paiement électronique, nombre de paiement électronique, contrôle de l'activité d'un magistrat particulier …

13. La Commission regrette de constater que, contrairement au souhait qu'elle a émis dans son avis sur les avant-projets de loi[4], cette finalité ne soit pas explicitée avec plus de précision afin de répondre aux exigences de la Cour européenne des droits de l'homme en matière de qualité et de précision de la loi. Le risque d'atteinte à la vie privée sur ce point a déjà été mis en évidence par la Commission.

14. Dès lors, s'il est envisagé que le système d'information Phenix soit interconnecté avec d'autres banques de données de l'administration, il importe que ces flux d'informations soient transparents et que les conditions, modalités et finalités de ces interconnexions soient précisées. A cet effet, la Commission recommande vivement au comité de gestion de Phenix d'apporter des **précisions sur ces interconnexions** (quelles banques de données, pour quelles finalités, dans quelles conditions et selon quelles modalités?), habilité pour ce faire en vertu l'article 17 de loi Phenix 1 à faire des propositions au Roi.

15. Il importe en effet qu'un **contrôle** de ces interconnexions soit rendu possible tant par la Commission que les personnes concernées. Un tel contrôle n'est possible que lorsqu'une publicité et une transparence des traitements sont réalisées.

2.2. L'utilisation du numéro d'identification du Registre national en tant qu'identifiant du citoyen[5] au sujet duquel des informations sont conservées dans le système d'information Phenix

16. Une étude approfondie sur les numéros personnels d'identification a été réalisée par le **Comité d'experts sur la protection des données** sous l'égide du Comité européen de coopération juridique.[6] Cette étude fait état tant des avantages (pérennité, simplification administrative, identification plus sûre que la seule utilisation du nom et du prénom) que des inconvénients (risque d'atteinte à la dignité humaine par la réduction des personnes physique à des numéros, interconnexion globale des fichiers administratifs, risque d'exclusion de la personne concernée des circuits d'information, risque d'anéantissement de l'anonymat des citoyens et de leur droit à l'autodétermination informationnelle) d'une utilisation d'identifiant global unique.

17. Parmi les conclusions de cette étude du Conseil de l'Europe figurent les principes suivants :

- « 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 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) »

---

[4] Avis n°11/2004, p. 80 et p.82.

[5] Par "citoyen", on entend ici toute personne physique, autre qu'un membre de l'organisation judiciaire ou qu'un collaborateur de la justice, dont des données à caractère personnel sont traitées dans le système d'information Phenix. Il peut par exemple s'agir de parties dans des affaires de droit civil, commercial et social (comme des requérants, des défendeurs, des intervenants volontaires forcés, des parties qui reprennent l'instance, …), d'inculpés, de personnes mises en accusation, de personnes condamnées, de parties civiles, de témoins, … Le "citoyen" est ainsi distingué des membres de l'organisation judiciaire et des collaborateurs de la justice, comme les avocats, les huissiers de justice ou les notaires, qui, dans l'exercice de leur fonction, voient leurs données à caractère personnel traitées à titre professionnel dans le système d'information Phenix.

[6] Disponible sur le site web du Conseil de l'Europe à l'adresse suivante :
http://www.coe.int/T/F/Affaires_juridiques/Coop%E9ration_juridique/Protection_des_donn%E9es/Documents/Publications/4Pins.asp#TopOfPage

18. Il convient également de relever que **l'article 8 de la Directive 95/46/CE**[7] traite des identifiants de portée générale sous la section des **catégories particulières de traitements au même titre que les données sensibles au sens des articles 6 à 8 de la loi vie privée**. Aux termes de l'article 8.7 de la directive, les Etats membres se sont par ailleurs engagés à déterminer les conditions dans lesquelles un numéro national d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement.[8]

19. L'utilisation du numéro de registre national présente bien entendu des **qualités administratives** telle que la pérennité, l'unicité ou encore la facilité d'utilisation pour les interconnexions généralisées. L'utilisation de ce numéro **en tant qu'identifiant unique** présente des **risques non négligeables** d'atteinte au droit au respect de la vie privée.

20. De nombreuses autorités de protection des données européennes et certains gouvernements européens ont, d'ores et déjà, posé à titre de principe l'obligation d'utilisation d'identifiants sectoriels (**Allemagne, France, Portugal, Grèce, Portugal, Pays-bas, Italie, Autriche**). A ce sujet, l'Autriche s'est également récemment illustrée à ce titre pour son modèle de « citizen cards » privacy compliant dans la mesure où seuls des identifiants spécifiques distinct par secteurs (Fisc, enseignement, santé…) sont utilisés et leur attribution est réalisée par une instance indépendante.

21. Il a été considéré par la Commission dans ses précédents avis[9] qu'il est conseillé de travailler avec des **identifiants sectoriels spécifiques** dans les **domaines sensibles.**

22. A l'occasion de son avis sur l'avant projet de loi Phenix (point 25 dudit avis), la Commission a d'ailleurs insisté sur le fait que les codes et clés d'accès aux dossiers judiciaires ne peuvent se référer directement ni aux noms des parties, ni à ceux de leurs représentants en justice.

23. Plusieurs collaborateurs de la justice ont déjà été autorisés, par arrêté royal ou, par autorisation du comité sectoriel du Registre national, à utiliser le numéro d'identification du Registre national. C'est notamment le cas dans :
    - l'arrêté royal du 30 septembre 1985 *autorisant les juges d'instruction, les magistrats du ministère public, les secrétaires en chef, les secrétaires chefs de service, les secrétaires, les secrétaires adjoints et les rédacteurs membres du personnel des parquets, des auditorats du Travail ou Militaires, à accéder au Registre national des personnes physiques et à utiliser le numéro d'identification du Registre national des personnes physiques* (modifié par l'A.R. du 4 avril 2003 et par l'A.R. du 7 juillet 2003) ;
    - l'arrêté royal du 14 mars 1991 *autorisant les greffiers des cours et tribunaux de l'Ordre judiciaire à accéder au Registre national des personnes physiques et à utiliser le numéro d'identification du registre national des personnes physiques ;*
    - l'arrêté royal du 14 avril 2002 *autorisant l'A.S.B.L. Fédération royale du Notariat belge à accéder aux informations du Registre national des personnes physiques et à en utiliser le numéro d'identification ;*
    - la délibération RN n° 06/2006 du 1er mars 2006 relative à la demande formulée par la Chambre nationale des huissiers de justice de Belgique, en son nom propre et au nom de ses membres, afin d'accéder aux informations du Registre national et d'utiliser le numéro d'identification dudit registre en vue, notamment, de l'exécution des articles 139 et 140 de la loi hypothécaire.

[7] Directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données.
[8] Cfr également les considérants 53 et 54 de la directive 95/46 y relatifs.
[9] Avis n°01/2005 du 10 janvier 2005, avis n°10/2004 du 23 septembre 2004, avis n°33/2002 du 22 août 2002, avis n°30/2002 du 12 août 2002, avis n°19/2002 du 10 juin 2002, avis n°14/2002 du 8 avril 2002.

24. Il convient toutefois de distinguer *la consultation* du Registre national *à des fins de vérification* des données d'identification centralisées audit Registre *de l'utilisation* du numéro de Registre national comme numéro d'identification unique des personnes. La vérification au Registre national des données d'identification par les collaborateurs de la Justice est bien-sûr nécessaire à l'accomplissement des tâches qui relèvent de leur compétence et c'est à ce titre qu'ils ont été autorisés. De cette manière, les greffiers peuvent consulter le Registre national des personnes physiques afin, par exemple, de connaître l'adresse actuelle d'un justiciable qui y est repris pour lui communiquer un acte de procédure.

25. Il importe également d'avoir égard à l'article 7 de la loi Phenix 1 qui prévoit que c'est **sans préjudice des dispositions de la loi du 8 août 1997 relative au casier judiciaire central** qu' « il est crée, au sein de Phenix, une banque de données de jurisprudence interne, afin de permettre le traitement des dossiers judiciaires par les différents membres d'une même juridiction, et une banque de données externe, destinée à diffuser dans le public les décisions ayant une importance pour la connaissance et l'évolution du droit »[10].

26. Au vu de ce qui précède, le **numéro de registre national** ne devrait pas être utilisé *de manière généralisée* en tant que numéro d'identification des justiciables au sein du système d'information **Phenix** dans la mesure où l'appareil judiciaire traite des données qualifiées de sensibles (art.8 LVP) et nécessitant une protection accrue en terme de protection des données. Il est souhaitable qu'un **numéro spécifique distinct du numéro de registre national** identifie les justiciables.

27. La Commission insiste pour que l'utilisation du numéro d'identification du Registre national dans le cadre du système d'information Phenix soit entourée d'un certain nombre de garanties. Il faut en effet éviter que l'utilisation du numéro d'identification du Registre national ait pour conséquence qu'il soit trop facile d'échanger ou de mettre en relation des données à caractère personnel d'une manière non conforme à la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après la « LVP ») et, en particulier, au principe de proportionnalité formulé à l'article 4, § 1, 3°, de ladite loi. Les données à caractère personnel traitées dans le système d'information Phenix étant principalement des données judiciaires, il est d'autant plus nécessaire de se prémunir contre des échanges / associations injustifiée(s) de données à caractère personnel.

28. La Commission estime, en outre, que l'article 4, § 1, 5°, de la LVP interdit de conserver le numéro d'identification du Registre national dans le système d'information Phenix si le dossier a été archivé et qu'il n'est, de ce fait, plus nécessaire de procéder au moindre échange légitime de données à caractère personnel. Il faut dès cet instant effacer le numéro d'identification du Registre national, de manière à exclure toute possibilité d'établir des liens entre dossiers actifs et dossiers archivés en se basant sur le numéro précité.

29. Ainsi que cela a déjà été indiqué plus haut, il importe, dès lors qu'il est envisagé d'interconnecter le système d'information Phenix avec d'autres banques de données de l'administration, que les flux d'informations soient transparents et que les conditions, modalités et finalités de ces interconnexions soient précisées. A cet effet, la Commission recommande formellement au comité de gestion de Phenix d'apporter des précisions au sujet de ces interconnexions (quelles banques de données, pour quelles finalités, sous quelles conditions et selon quelles modalités?). En vertu de l'article 17 de la loi Phenix 1, le comité de gestion est habilité à faire des propositions au Roi à ce propos. Il importe en effet qu'un contrôle puisse être exercé sur ces interconnexions, tant par la Commission que par les personnes

[10] Il ressort par ailleurs des débats qui ont eu lieu en Commission Justice du Sénat sur ce point que le délégué de la Ministre de la Justice a d'ailleurs déclaré que la finalité de la banque de jurisprudence interne de Phenix consiste uniquement à permettre aux membres d'une juridiction entendue au sens strict d'assurer une certaine unité de jurisprudence et ainsi de permettre à un magistrat du travail de retrouver toutes les décisions déjà prises par lui dans un type d'affaires et le cas échéant de reproduire la motivation et le dispositif y repris. (doc Sénat n°3/1163/3)

concernées. Un tel contrôle n'est possible que si la publicité et la transparence des traitements sont assurées.

30. Il va de soi qu'il n'est pas permis d'utiliser le numéro d'identification du Registre national dans le cadre de la banque de données de jurisprudence externe, ni dans celui de l'élaboration de statistiques. En vertu des articles 9, 10 et 12 de la loi du 10 août 2005 *instituant le système d'information Phenix*, les données utilisées à ces fins doivent être anonymisées ou codées.

31. La Commission constate dès lors avec satisfaction que des mesures techniques sont entreprises à ce niveau afin d'utiliser un tel numéro spécifique et d'empêcher toute recherche généralisée au sein de Phenix sur base du numéro de registre national d'une personne physique. A ce titre, les auteurs du projet pourraient, le cas échéant, s'inspirer des travaux menés à ce niveau au sein du projet Bhealth (Dossier médical informatisé) par le Professeur De Moor de l'université de Gand[11].

32. Si la voie du cryptage du numéro de registre national des personnes physiques devait être choisie par les auteurs du projet Phenix, il importe que des garanties spécifiques soient prévues afin que les clefs de décryptage soient accessibles et utilisées uniquement par les seules personnes habilitées moyennant le respect des dispositions légales en la matière et pour des finalités déterminées et précises et transparentes tant pour la Commission que pour les justiciables.

33. En conclusion, le numéro de Registre national peut être enregistré sous forme chiffrée (cryptée) dans le système phenix mais ne peut être une clef d'identification dans le système lui-même. Il convient donc que l'utilisation dans le système phenix du numéro de registre national soit explicitement prévue dans le cadre des AR d'exécution de phenix. Il conviendra d'expliciter quelles seront les personnes habilitées à détenir les clefs de déchiffrement et pour quelles finalités légitimes, proportionnelles et transparentes l'échange ou la mise en relation de fichiers pourra être réalisé sur base de ce numéro et moyennant le respect des dispositions légales en la matière.

3. AUTHENTIFICATION DES PERSONNES AYANT ACCES AU SYSTEME D'INFORMATION PHENIX ET UTILISATION DE LA CARTE D'IDENTITE ELECTRONIQUE POUR CETTE FINALITÉ

34. En raison du caractère particulièrement sensible des données y traitées, l'accès au système d'information Phenix doit être très bien protégé. Dans ce cadre, il est essentiel que chaque utilisateur puisse être authentifié d'une manière ne laissant subsister aucune équivoque et que la qualité (par ex. juge, greffier, avocat, …), en vertu de laquelle un utilisateur a accès au système, puisse être vérifiée de façon probante. Par authentification, on entend le processus permettant de s'assurer que l'identité déclinée par un utilisateur en vue d'accéder au système d'information Phenix est bien la sienne. L'authentification peut se faire sur la base d'informations que l'utilisateur est censé détenir (par ex. un mot de passe), d'une chose censée être en sa possession (par ex. un certificat mémorisé sur une carte pouvant être lue électroniquement), de caractéristiques biométriques ou d'une combinaison de plusieurs de ces moyens. En l'espèce, il semble indispensable que l'authentification repose au minimum sur la vérification combinée des deux premiers moyens cités. Le demandeur d'une session devra donc impérativement disposer d'un ensemble de clés (userid, password, et clé personnelle) La vérification de la qualité est le processus permettant de vérifier qu'un utilisateur possède effectivement la qualité dont il se prévaut pour avoir accès à certaines parties du système d'information Phenix. Cette vérification peut être effectuée en recourant à des moyens analogues à ceux utilisés pour l'authentification d'un utilisateur ou, après avoir procédé à l'authentification, en consultant une banque de données authentiques dans laquelle sont enregistrées les qualités dont peut se prévaloir l'utilisateur identifié ou par le biais de l'utilisation de certificat électronique d'authentification professionnelle.

[11] Cfr à ce sujet **http://www.health-telematics.be/behealth/20060120-bvt-gdm.pps**

35. La Commission estime cependant que tous les moyens qui peuvent être utilisés pour l'authentification de l'identité et les certificats qui seraient utilisés pour prouver une qualité pertinente et qui seraient repris sur une carte professionnelle doivent répondre aux exigences strictes prévues pour les certificats qualifiés au sens de la loi susmentionnée du 9 juillet 2001.

36. Bien entendu, avant de mettre à la disposition d'un utilisateur les moyens qui lui permettront de se faire authentifier et de prouver sa qualité, il faut établir avec une certitude suffisante l'identité et la qualité en question (en organisant par exemple un contrôle « face to face »).Autrement, un utilisateur pourrait trop aisément se fabriquer une fausse identité ou une fausse qualité. Le processus d'enregistrement de l'identité et des qualités doit donc être conçu de manière à lever tout doute à ce sujet.

37. La Commission constate que le certificat enregistré à des fins d'authentification sur la carte d'identité électronique satisfait aux normes sévères prévues quant aux certificats qualifiés par la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification. Les exigences relatives aux certificats précités – aussi bien celles se rapportant aux certificats eux-mêmes (annexe I de la loi) que celles ayant trait aux prestataires de service de certification qui les délivrent (annexe II) et celles concernant les dispositifs sécurisés de création de signature électronique (annexe III) – ont été respectées pour les certificats d'authentification, à la seule exception des éléments indissociables de la signature qui ne peuvent pas être utilisés en vue de l'authentification.

38. La Commission estime que le certificat d'authentification présent sur la carte d'identité électronique offre les garanties nécessaires pour l'authentification de l'identité d'un utilisateur du système d'information Phenix. Etant donné que ce certificat ne comporte cependant pas la preuve d'une qualité, cette dernière peut être vérifiée à l'aide d'une banque de données authentiques dans laquelle la qualité pertinente est enregistrée et gérée en collaboration avec les sources authentiques de ces qualités que constituent les différents ordres professionnels concernés, s'ils existent. Dans ces bases de données, les numéros de registre national des membres pourront être repris afin que soit établi le lien entre ledit numéro et la qualité de son titulaire.

39. Quant à l'opportunité ou non d'imposer l'utilisation de la carte d'identité électronique, s'il convient de distinguer la fonction d'identification traditionnelle de la carte d'identité de ses deux nouvelles fonctions que constituent l'authentification électronique[12] et la signature électronique[13] [14], la Commission relève **qu'en vertu de l'article 6, §7 [15] de la loi précitée du 19 juillet 1991**, **il appartient également au Roi, après avis de la Commission, de déterminer, en plus des autorités et officier public sur la réquisition desquels la carte d'identité doit être présentée**[16]**, les modalités d'utilisation de la carte d'identité**.

---

[12] Processus actif par lequel le porteur d'une carte d'identité électronique s'identifie de façon volontaire et électronique. Cela est attesté par le certificat électronique fourni par Certipost en tant que tiers de confiance ayant pour mission la délivrance et la gestion des certificats d'authentification et de signature électroniques de la carte d'identité

[13] Le processus technique de la signature électronique est identique à celui de l'authentification électronique à la différence que dans le processus de signature électronique, c'est un message sémantique qui est chiffré alors dans le processus d'authentification,c'est un nombre aléatoirement crée par la carte qui est chiffré.

[14] Le rapport au Roi précédant l'AR du 25 mars 2003 fait à cet égard également la distinction entre les différentes fonctionnalités de la carte d'identité électronique. On peut y lire qu'en cas d'utilisation de la carte d'identité à distance, seul l'aspect authentification et signature électronique est utilisable et que les différentes données d'identité ne sont ni visibles à l'œil nu ni lisible de manière électronique. De plus, le rapport au Roi semble se baser sur la nécessité du **consentement** du titulaire pour la captation électronique des données d'identité reprises à l'article 6 de la loi du 19 juillet 1991.

[15] Art 6 § 7 L 19/07/1991 "Le Roi détermine, après avis de la Commission de la protection de la vie privée, instituée par la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, la forme et les modalités de fabrication, de délivrance **et d'utilisation** de la carte d'identité.

[16] Tel que prévu à l'article 1er de l'AR du 25/03/2003 relatif aux cartes d'identité.

40. Une généralisation inconditionnée et non justifiée de cette utilisation apparaitrait contraire aux principes de finalité, de proportionnalité et de légitimité de la loi vie privée ainsi qu'au Rapport au Roi précédant l'AR du 25 mars 2003

41. A ce sujet, il conviendrait également que le législateur s'interroge sur les **risques de créer** une **extension de l'utilisation de la carte d'identité à toutes les sphères d'activités de la vie d'un individu** alors que la carte d'identité n'a jusqu'à ce jour été confinée qu'à la sphère intime de l'individu et non à sa sphère de vie professionnelle.

42. De plus, tous les utilisateurs du système d'information Phenix ne disposent pas d'une carte d'identité électronique. On pense notamment aux avocats étrangers. En outre, chaque titulaire d'une carte d'identité électronique est libre de ne pas activer les certificats sur sa carte, conformément à l'article 6, § 2, dernier alinéa de la loi du 19 juillet 1991 *relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques*.
La Commission estime d'ailleurs qu'il n'est pas souhaitable qu'un utilisateur du système d'information Phenix soit obligé d'utiliser sa carte d'identité électronique pour l'authentification de son identité à l'égard du système d'information Phenix.

43. Enfin, il ressort de l'article 6, § 2 de la loi du 19 juillet 1991 que le choix de recourir à un prestataire de service de certification accrédité pour la carte d'identité électronique a été opéré par le législateur[17]. Jusqu'à présent, il apparaît qu'aucun prestataire de service de certification accrédité n'ait reçu d'accréditation. En vertu de la Directive européenne 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 *sur un cadre communautaire pour les signatures électroniques* et de la loi du 9 juillet 2001 *fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification*, l'accréditation du prestataire de service de certification ne constitue pas une condition pour la validité des signatures. Une signature avancée, conçue au moyen d'un dispositif sécurisé de création de signature, basé sur un certificat qualifié délivré par un prestataire de service de certification qui satisfait aux conditions de l'annexe II de la loi, constitue une signature valable produisant les mêmes effets qu'une signature manuscrite. Toutefois, la loi du 19 juillet 1991 *relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques* mentionne qu'il s'agit, dans le cas des certificats sur la carte d'identité électronique, d'un prestataire de service de certification accrédité. Bien que l'accréditation n'ait strictement aucune influence sur la validité de la signature, la Commission estime que la loi doit être respectée.

4. CONSTITUTION DES LISTES PROFESSIONNELLES

44. La Ministre de la Justice interroge également la Commission sur la façon dont les listes professionnelles des acteurs de Phenix peuvent être créées.

45. Afin de pouvoir réaliser une authentification forte (décrite au point 40) des acteurs au sein de Phenix, le projet de loi relatif à la procédure par voie électronique prévoit en ses articles 23 à 25 et en son article 53 l'établissement de **listes professionnelles** qui seront **publiques**.

46. Conformément à l'article 4 de la loi vie privée, il importe que ces listes soient constituées uniquement de données pertinentes et non excessives afin de réaliser la finalité qui est de s'assurer de la qualité d'un auxiliaire de justice. S'il s'agit d'identifier uniquement la fonction d'une personne, il importe que soient reprises dans cette liste uniquement les données nécessaires à cet effet à savoir **le nom, le(s) prénom(s), la qualité de l'auxiliaire de justice ainsi que son ou ses adresse(s) professionnelle(s) et, le cas échéant, son adresse**

[17] L'article 17 de la loi du 9/07/2001 prévoit en effet une procédure d'accréditation volontaire pour les prestataires de service de certification accrédités, attribuant pour ainsi dire un label de qualité à ces prestataires de service, après contrôle par l'administration. Ce label de qualité confirmerait ainsi la conformité du prestataire de service avec les conditions des annexes de la loi, et donc entre autres en ce qui concerne les données comprises dans le certificat.

judiciaire électronique. D'autres données non pertinentes devraient dès lors faire l'objet du consentement des personnes concernées.

5. IDENTIFICATION DES MEMBRES DE L'ORGANISATION JUDICIAIRE ET DES COLLABORATEURS DE LA JUSTICE AU SEIN MÊME DU SYSTEME D'INFORMATION POUR DES FINALITÉS AUTRES QUE LE CONTRÔLE D'ACCÈS ET LA CRÉATION DE LOGINS

47. Selon les informations obtenues par la Commission sur l'état actuel de l'architecture du système d'information, les membres de l'organisation judiciaire, les avocats et les auxiliaires de la justice, une fois passés les contrôles d'accès (tels que décrits ci-dessus) et exception faite de l'identification dans les loggins selon le choix du groupe professionnel concerné, pourront être identifiés au sein-même du système d'information au choix soit à l'aide du numéro d'identification du Registre national, soit à l'aide d'un numéro d'identification spécifique. C'est ainsi qu'un **numéro d'identification spécifique** pourrait être utilisé pour les avocats (numéro d'avocat unique se substituant un numéro de registre national de l'avocat), ou pour les membres de l'Ordre judiciaire (le numéro de matricule pour les magistrats, greffiers,…) .

48. Etant donné les considérations de la Commission formulées ci-dessus, la Commission estime que l'utilisation au sein de Phenix d'un tel identifiant sectoriel pour certains groupes professionnels constitue un moyen utile pour appliquer aux identifiants le principe de proportionnalité repris à l'article 4 de la LVP, pour autant que cela soit techniquement possible et ne compromette en rien le niveau de sécurité de Phenix.

6. UTILISATION DE LA SIGNATURE ELECTRONIQUE DANS LE SYSTEME D'INFORMATION PHENIX ET UTILISATION DE LA CARTE D'IDENTITÉ ELECTRONIQUE A CET EGARD.

49. La loi du 9 juillet 2001 *fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification* détermine les conditions selon lesquelles une signature électronique implique automatiquement les mêmes conséquences juridiques qu'une signature manuscrite.

50. L'article 4, § 4 de ladite loi dispose qu'une signature électronique avancée, réalisée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique, est assimilée à une signature manuscrite. Une telle signature électronique est appelée une signature électronique qualifiée et est considérée comme étant suffisamment sûre pour être assimilée automatiquement à une signature manuscrite sans que le juge ne doive vérifier à cet égard si les garanties de sécurité requises sont présentes.

51. Un certificat qualifié est, selon la loi, un certificat qui satisfait aux exigences visées à l'annexe I de ladite loi et qui est fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II de cette même loi. Le prestataire de service de certification des certificats de la carte d'identité électronique, Certipost, a, conformément à l'article 4 § 2 de la loi précitée du 9 juillet 2001, déclaré au SPF Mineco délivrer des certificats qualifiés. La liste des prestataires de services de certification délivrant de tels certificats est publiée sur le site web du SPF Mineco.

52. L'**article 5**[18] **de ladite loi** prévoit que tout prestataire de service de certification délivrant des certificats à l'intention du public ne peut recueillir des données à caractère personnel que par la **collecte directe** auprès de la personne concernée **ou** moyennant le **consentement explicite** de celle-ci **et uniquement dans la mesure où cela est nécessaire à la délivrance et à la conservation du certificat**.

53. De plus, l'**annexe 1** de la loi "signatures électroniques" décrit les données que doit comporter tout certificat qualifié. Parmi ces données, figure la possibilité d'inclure, le cas échéant, une **qualité spécifique** du signataire, en fonction de l'usage auquel le certificat est destiné.

54. La loi considère que l'utilisation d'un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la création de signature qui satisfait aux exigences de l'annexe III de cette même loi constitue un dispositif sécurisé de création de signature. La carte à puce, qui constitue le support de la carte d'identité électronique, y satisfait.
55. La signature électronique avancée est définie comme suit à l'article 2, 2° :
"une donnée électronique, jointe ou liée logiquement à d'autres données électroniques, servant de méthode d'authentification et satisfaisant aux exigences suivantes :
a) être liée uniquement au signataire ;
b) permettre l'identification du signataire ;
c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectée."

56. La Commission relève que le certificat de signature électronique de la carte d'identité électronique est implémenté de telle façon que **sont systématiquement communiqués au destinataire d'un document signé électroniquement à l'aide de la carte d'identité électronique: le nom, les deux premiers prénoms ainsi que le numéro de registre national du titulaire de la carte**[19] (le numéro de registre national étant utilisé comme numéro de série des certificats de la carte d'identité électronique).

57. **La Commission s'interroge sur ce point et désirerait connaître la raison d'être de cette communication systématique du n° de Registre national en plus des nom et deux premiers prénoms.**

58. La Commission souligne que l'utilisation ultérieure du numéro d'identification du Registre national par le destinataire du certificat de signature est soumise, sauf dans les cas déterminés par le Roi par arrêté délibéré en Conseil des Ministres après avis du comité sectoriel du Registre national, à une autorisation du comité sectoriel du Registre national. Le numéro d'identification du Registre national repris sur le certificat de signature intégré à la carte d'identité électronique ne peut ainsi, dans l'état actuel de la réglementation, être traité ultérieurement que par des instances habilitées à cet effet. Les instances qui ne disposent pas d'une telle autorisation et à l'égard desquelles une signature électronique est apposée sur la base de la carte d'identité électronique ne peuvent pas traiter ultérieurement le numéro d'identification du Registre national. Au niveau technique, il convient de veiller à ce que le certificat ne soit, dans ce cas, utilisé que pour la validation de la signature électronique, en

[18] "Art. 5.§ 1er. Sans préjudice de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, un prestataire de service de certification qui délivre des certificats à l'intention du public ne peut recueillir des données personnelles que directement auprès de la personne concernée ou avec le consentement explicite de celle-ci et uniquement dans la mesure où cela est nécessaire à la délivrance et à la conservation du certificat. Les données ne peuvent être recueillies ni traitées à d'autres fins sans le consentement explicite de la personne intéressée.
§ 2. Lorsque le titulaire du certificat utilise un pseudonyme et lorsque les nécessités de l'instruction l'exigent, le prestataire de service de certification ayant délivré le certificat est tenu de communiquer toute donnée relative à l'identité du titulaire dans les circonstances et selon les conditions prévues par les articles 90ter à 90decies du Code d'instruction criminelle."
[19] Newsletter n°1 sur la carte d'identité électronique disponible sur le site Internet du Ministère de l'Intérieur (Registre national)

excluant tout traitement ultérieur. En vue de la preuve, il ne faut conserver que ce qui peut être considéré comme adéquat, pertinent et non excessif, conformément à l'article 4, §1, 3° de la LVP.

59. L'article 4, § 3 de la loi du 9 juillet 2001 dispose que le Roi peut, par arrêté délibéré en Conseil des Ministres, soumettre l'usage des signatures électroniques dans le secteur public à des exigences supplémentaires éventuelles. Ces exigences doivent être objectives, transparentes, proportionnées et non discriminatoires et ne s'appliquer qu'aux caractéristiques spécifiques de l'application concernée. Elles ne peuvent pas constituer un obstacle aux services transfrontaliers. Sans préjudice des interrogations de la commission sur la configuration actuelle des certificats, cet article peut constituer la base d'une réglementation imposant les exigences de sécurité pour la signature lors de l'utilisation de la signature électronique dans le cadre du système d'information Phenix.

60. Il ressort des articles 7 et 2 3° du projet de loi Phenix 2 que la seule obligation imposée aux futurs utilisateurs de Phenix concernant la signature électronique soit l'utilisation de la signature électronique qualifiée. Le choix semble légitime car une telle signature électronique est la seule à bénéficier du principe d'assimilation automatique à la signature manuscrite en raison des garanties de sécurité qui y sont associées. Une signature électronique apposée à l'aide de la carte d'identité électronique constitue une signature électronique qualifiée. Des signatures électroniques qualifiées apposées à l'aide de moyens autres que la carte d'identité électronique doivent cependant également être possibles.

61. La Commission considère que **l'utilisation de certificat des signatures électroniques professionnelles pourrait être envisagée** dans la mesure où cette solution présente l'avantage, d'une part, d'atteindre la finalité voulue qui est de signer électroniquement tout en attestant de sa qualité spécifique sans que le numéro de registre national ne soit utilisé et, d'autre part, d'éviter une extension de l'utilisation de la carte d'identité à la sphère professionnelle**.** De tels certificats pourraient, en effet, attester de la qualité professionnelle spécifique d'un signataire.

62. Ces certificats pourraient être gérés par un **tiers de confiance** en collaboration avec les organisations professionnelles concernées. Ce tiers de confiance peut le cas échéant, être le prestataire de service de communication[20] dont les activités sont réglementées par le projet de loi Phenix 2 dans la mesure où il résulte de l'article 10 §1er 2° qu'il lui appartiendra de « vérifier, par des moyens appropriés et légaux, l'identité des parties à la signification, à la notification ou à la communication ».

PAR CES MOTIFS,

La Commission, émet un avis favorable dans la mesure où les mesures techniques requises sont mise en œuvre afin qu'un numéro d'identification sectoriel spécifique, distinct du numéro de Registre national (cfr supra point 33), soit utilisé pour les justiciables dans le but notamment d'éviter toute recherche sur base du numéro de Registre national ;

En réponse aux questions qui lui ont été posées, la Commission recommande :

- que des mesures soient prises en vue de l'utilisation de certificats électroniques professionnels qui présentent les avantages décrits au point 61;

[20] l'article 2 4° du projet de loi Phenix 2 définit lesdits prestataires comme étant toute « entreprise répondant aux conditions fixées à l'article 10 de la présente loi, ainsi qu'à celles fixées par le Roi, après avis du comité de gestion et du comité de surveillance, intervenant comme organe intermédiaire lors d'une signification, d'une notification, d'un dépôt ou d'une communication dans le cadre d'une procédure judiciaire ».

- l'intervention du législateur pour que soient précisées les modalités d'utilisation de la carte d'identité;
- que les listes professionnelles publiques soient uniquement constituées de données pertinentes, les autres devant être légitimées par le consentement des personnes concernées.

L'administrateur, Le président,

(sé) Jo BARET (sé) Michel PARISSE