La justice au risque de la vie privée

Poullet, Yves

Published in:
Phénix et la procédure électronique

Publication date:
2006

Document Version
le PDF de l'éditeur

2

La justice au risque de la vie privée

Yves POULLET [1]
professeur aux F.U.N.D.P. et à U.Lg.
directeur du C.R.I.D.

Damien MOREAU [2]
collaborateur scientifique au C.R.I.D.

1. Ancien membre de la Commission de protection de la vie privée, rapporteur lors de l'avis n° 11/2004 de la Commission vie privée relatif au système Phenix.

2. Conseiller-scientifique au C.R.I.D. ; juriste-légiste au S.P.F. Justice, DG législation ; rédacteur de la loi du 10 août 2005 instituant le système d'information Phenix.

L'article n'engage que ses auteurs.

Nos remerciements à S. RANS, J.M. KARUIJE et F. DANIELI, et aux autres collègues du service.

sommaire

Introduction

1 L'article 2, alinéa 1 de la loi du 10 août 2005 instituant le système Phenix dispose :

> « Il est créé un système d'information appelé Phenix qui a pour finalités 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, l'élaboration de statistiques et l'aide à la gestion et l'administration des institutions judiciaires ».

La disposition est révolutionnaire à plus d'un endroit, ajoutera-t-on. Si l'informatique avait déjà quelque peu — et non sans difficultés — risqué un premier pas dans nos augustes et vénérables prétoires [3], l'ambition de Phenix entend imposer les technologies modernes de l'information et de la communication comme une seconde nature de l'appareil judiciaire.

---

3. Ainsi, J. HUBIN (« Les relations Barreau-Palais : la diffusion des données jurisprudentielles dans le cadre du programme "Phenix" d'informatisation de l'ordre judiciaire », in *Cabinets d'avocats et Technologies de l'information*, J.F. Henrotte, Y. Poullet (éd), in Cahiers du C.R.I.D. n° 26, Bruxelles, Bruylant, 2005, p. 335 et note 46) cite I. VEROUGSTRAETE : « *Les investissements dans l'équipement informatique depuis le début des années 90 ont été importants, mais inefficaces. Avec les programmes successifs du département de Justice, plusieurs éléments ou niveaux dans le pouvoir judiciaire ont été pourvus de matériel et de logiciel à l'appui de la procédure. Les magistrats et les greffiers ont également lourdement investi à leurs propres frais dans l'informatisation de leurs activités et ils ont parfois fabriqué des applications qui sont actuellement encore utilisées des les cours et tribunaux* ».

« *Le résultat final n'est pas satisfaisant, et non seulement parce que les systèmes existants ne sont pas compatibles, il en résulte beaucoup de travail inutile. Le niveau de développement est très divergent — certaines branches se trouvent encore au point zéro, tandis que d'autres se trouvent au niveau de systèmes WP archaïques — et le tout est extrêmement coûteux en ce qui concerne les prix de l'entretien et des licences* ».

Il n'est pas un pas que le justiciable accomplira dans l'enceinte judiciaire, devenue virtuelle pour la cause, sans que l'ordinateur ne le guide. Il n'est pas une opération que le membre du pouvoir judiciaire n'accomplira sans le concours de cette technologie. L'efficacité, la rapidité, mais également la plus grande transparence autant d'arguments invoqués autour du berceau de Phenix [4] et bénis d'ailleurs par les instances internationales [5].

2 Mais cette révolution du Palais n'est pas celle que nous souhaitons souligner aujourd'hui. Une réflexion du Conseil d'État invite en effet à un second propos. À la version présentée à sa lecture [6] qui notait : « *Il est créé un système d'information appelé Phenix, qui a pour objectifs...* », le Conseil d'État [7] présente l'observation suivante :

> « Il conviendrait de remplacer les termes "qui a pour objectif" par les termes "qui a pour finalités" afin de mieux s'inscrire dans le cadre des directives communautaires et plus particulièrement de la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, modifiée par le règlement (CE) n° 1882/2003 du Parlement européen et du Conseil du 29 septembre 2003 ainsi que de la loi du 8 décembre 1992 précitée ».

Ainsi, la « Vie privée » entre en même temps que les ordinateurs et les câbles dans la vie de nos juridictions.

Mieux, elle en structure l'action et impose au pouvoir judiciaire sa loi. La communication entre magistrats, celle du Palais avec le monde extérieur, la diffusion de la production judiciaire, la réalisation d'opérations statistiques sont devenues autant de traitements de données à caractère personnel soumis à l'article 8 de la Convention européenne des droits de l'Homme, à l'article 22 de la Constitution, à la loi du 8 décembre 1992 [8] et à son arrêté d'exécution.

3 La révolution est de taille. Sans doute, les juges appliquaient-ils — rarement, il est vrai — cette loi [9]. Ils se découvrent soudain « soumis », « contraints » par une législation qui dicte des limites tout à la fois à l'ensemble du pouvoir judiciaire qu'ils incarnent, qu'à leurs propres actions.

Sans doute, jusque là, habitués à des procédures papiers rigoureusement encadrées par le Code judiciaire et le Code d'instruction criminelle, procédures qu'ils suivaient solitaires ou entourés de leurs seuls greffiers dans un dialogue singulier avec les auxiliaires de justice, ils avaient pris peu conscience qu'ils opéraient des traitements au sens de la loi du 8 décembre 1992, c'est-à-dire « *Toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel* ».

4. On citera à ce propos les conclusions du Rapport de la Commission « Citoyen-Droit et Société » remis à la Fondation Roi Baudouin » (Rapport *À qui de droit : vers une relation de qualité entre le citoyen, le droit et la société*, 2001, p. 149) :
« *La justice fasse un usage accru des nouvelles technologies. L'objectif d'une justice performante suppose en effet que l'on fasse le plus grand usage possible des nouvelles technologies techniques qui sont aujourd'hui disponibles. C'est important pour travailler de manière non seulement plus rapide mais aussi plus efficace, par exemple dans la lutte contre des formes modernes de criminalité* ».

5. Ainsi la formule utilisée par la Recommandation Rec. (2001) 2 du Comité des ministres du Conseil de l'Europe concernant la conception et la reconception rentables des systèmes judiciaires et des systèmes d'information juridique (28 fév. 2000) et Rec. (2001) 3 sur les services des tribunaux et d'autres institutions juridiques fournis aux citoyens par les nouvelles technologies : « *Considérant que les nouvelles technologies d'information sont devenues un outil indispensable pour l'administration efficace des États européens notamment pour l'administration de la justice, favorisant ainsi le bon fonctionnement de la démocratie* ».

6. Publié dans le document parlementaire Doc 1645/001, p. 28.

7. L'avis du Conseil d'État n° 37.943/2 rendu le 11 janvier 2005 est publié également *eod. loco*, p. 43. À noter dans le même sens, mais nul ne s'en étonnera, l'avis de la Commission de protection de la vie privée n° 11/2004 du 4 octobre 2004 (Rapporteur Y. Poullet).
« Le premier avant-projet dit "Juricontrol" définit les multiples finalités de ce système d'information dit "Phenix" ».

8. Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993.

9. Même s'il faut bien noter le nombre croissant de recours fondés sur la loi du 8 décembre 1992. À cet égard, la contribution d' Y. Poullet in Y. Poullet, A. Cruquenaire, N. Daubies, D. De Roy, S. Dusollier, T. Lambert, J.F. Lerouge, C. Steyaert, A. Willems, *Droit de l'informatique et des technologies de l'information, Chronique de jurisprudence* 1995-2001, Les dossiers du Journal des tribunaux, n° 41, Larcier, 2003, en particulier n^{os} 143 et s.

4 Le partage d'informations au sein d'un réseau, l'accès à des ressources communes et la multiplication des connexions ne permettent plus d'occulter les risques que de telles opérations font courir à ceux que la loi déjà citée qualifie de personnes concernées.

Mais qui sont ces « personnes concernées ». Sans doute, évoquera-t-on tout d'abord les « justiciables » dont le nom évoqué à de multiples endroits et procédures en cours ou de décisions rendues permet de dessiner leur profil de justice.

Ainsi, cette personne condamnée pour un accident de roulage est en même temps celle qui a battu sa femme, introduit une instance contre son employeur et qui figure dans la centrale négative des crédits à la consommation. Le risque est, ajoutera-t-on, d'autant plus grand, que la plupart des données traitées constituent des données « judiciaires » au sens de la loi du 8 décembre 1992, c'est-à-dire des données sensibles dont la loi entoure le traitement de garanties particulières [10].

10. Art 8 de la loi du 8 décembre 1992 :
« § 1er — Le traitement de données à caractère personnel relatives à des litiges soumis aux cours et tribunaux, ainsi qu'aux juridictions administratives, à des suspicions, des poursuites ou des condamnations ayant trait à des infractions ou à des sanctions administratives ou des mesures de sûreté est interdit.
§ 2 — L'interdiction de traiter les données à caractère personnel visées au paragraphe 1er n'est pas applicable aux traitements effectués :
a) sous le contrôle d'une autorité publique ou d'un officier ministériel au sens du Code judiciaire, lorsque le traitement est nécessaire à l'exercice de leurs tâches ;
b) par d'autres personnes lorsque le traitement est nécessaire à la réalisation de finalités fixées par ou en vertu d'une loi, d'un décret ou d'une ordonnance ;
c) par des personnes physiques ou par des personnes morales de droit public ou de droit privé pour autant que la gestion de leurs propres contentieux l'exige ;
d) par des avocats ou d'autres conseils juridiques, pour autant que la défense de leurs clients l'exige ;
e) pour les nécessités de la recherche scientifique, dans le respect des conditions fixées par le Roi par arrêté délibéré en Conseil des ministres, après avis de la Commission de la protection de la vie privée.
§ 3 — Les personnes qui, en vertu du paragraphe 2, sont autorisées à traiter les données à caractère personnel visées au paragraphe 1er, sont soumises au secret professionnel.
§ 4 — Le Roi fixe, par arrêté délibéré en Conseil des ministres, après avis de la Commission de la Protection de la vie privée, les conditions particulières auxquelles doit satisfaire le traitement de données à caractère personnel visées au paragraphe 1er. »

L'auxiliaire de justice lui-même devient « personne concernée » à la faveur des traces, que ces demandes d'accès ou paiements électroniques ou ces échanges télématiques avec le Palais laissent quelque part sur le serveur de Phenix. Ainsi, peut-on enregistrer la fréquence de ses demandes, la tentative d'accéder au dossier d'un confrère, le refus d'un paiement électronique.

Et le magistrat, enfin, le voilà soumis à la surveillance électronique, au contrôle de son activité, de ses visites sur Internet.

Bref, tout devient traitement et toute personne de la justice soumise à elle, en contact avec elle, ou l'incarnant est qualifiable de personne concernée.

5 L'ordinateur ou plutôt le système d'information Phenix ne se contente pas d'amener avec lui la loi « Vie privée », il introduit également les « garants » de cette loi ; la Commission de protection de la vie privée entend ainsi exercer son rôle, faisant fi de l'indépendance du pouvoir judiciaire et oblige à trouver des compromis acceptables entre cette double exigence constitutionnelle : l'une affirmée par l'article 22 qui prescrit le respect du principe de la vie privée [11] et l'autre consacrant l'indépendance du pouvoir judiciaire.

Le compromis devient plus difficile encore lorsqu'il faut bien reconnaître la présence d'un troisième larron : le pouvoir exécutif ou pour être plus précis l'administration du S.P.F. Justice. La gestion et le développement du système d'information ne peuvent en effet s'imaginer sans l'intervention financière, technique et de gestion d'une administration dont le tout technologique rend la présence bien plus nécessaire encore.

La loi du 10 août 2005 tente de réaliser ces compromis par la création d'organes à la composition savamment dosée et en leur attribuant des compétences qui cherchent à ménager — non sans être l'objet de critiques — les objectifs constitutionnels parfois contradictoires.

Ce sera l'objet de notre premier titre. Le second analysera au regard de la loi de 1992, les dispositions décrivant les finalités du système d'information Phenix.

11. *« Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi. »*
« La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit. »

SECTION 1

Les organes mis en place par la loi Phenix et leurs compétences au regard du principe de la séparation des pouvoirs

6 À l'instar des autres grandes banques de données nationales, telles que le registre national, la banque carrefour de la sécurité sociale et la banque-carrefour des entreprises, la loi du 10 août 2005 instaure trois comités : un comité de gestion, un comité de surveillance et un comité d'utilisateurs.

Néanmoins, Phenix, à la différence des autres banques de données nationales, qui sont des banques de données appartenant à l'exécutif, est un système d'information gérant les dossiers judiciaires.

La composition et les modes de désignation et de fonctionnement des organes de Phenix diffèrent dès lors de ceux des autres banques de données, en ce qu'ils tentent d'établir un équilibre entre le pouvoir exécutif et judiciaire, voire même législatif dans la mesure où le comité de surveillance est institué auprès de la Commission vie privée, elle-même instituée auprès du Parlement.

A. Le comité de gestion

7 Comme son nom l'indique, le comité de gestion de Phenix a pour mission de gérer le système Phenix au quotidien.

Le comité de gestion est composé d'un président, d'un vice-président, de huit membres effectifs et de huit membres suppléants, désignés par le

Roi, par arrêté délibéré en Conseil des ministres, pour moitié sur proposition du ministre de la Justice et pour moitié sur proposition conjointe du premier président et du procureur général près de la Cour de cassation [12].

Le président et le vice-président exercent chacun leur fonction durant trois ans et puis l'échangent [13].

Le président et le vice-président du comité d'utilisateurs siègent également dans le comité de gestion avec voix consultative [14].

8 En ce qui concerne la qualité des membres, « *le président et le vice-président sont choisis parmi les personnes offrant toutes garanties d'indépendance et possédant des compétences notoires dans le domaine du droit de l'informatique* » [15]. La loi ne définit cependant pas ce qu'est une compétence notoire. Par contre, elle dispose que l'un des deux soit magistrat de l'Ordre judiciaire [16].

Parmi les membres désignés par la Cour de cassation, six au moins doivent être des membres de l'Ordre judiciaire, dont deux appartenant à un parquet ou un auditorat de première instance, un à une juridiction d'appel ou de cassation, un au siège d'une juridiction de premier degré, un au greffe et un au secrétariat des parquets. La Cour de cassation est par contre libre de proposer les deux membres restant parmi des personnes n'ayant pas la qualité de membres de l'Ordre judiciaire.

La loi n'impose aucune condition à l'égard des personnes proposées par le ministre de la Justice et celui-ci est donc libre de proposer des membres de l'Ordre judiciaire, des auxiliaires de justice (avocats, notaires, huissiers), des académiques ou des personnes sans titre ni qualités particulières [17].

12. Art. 15.
13. Art. 15, § 2, al. 2.
14. Art. 15, § 7.
15. Art. 15, § 2, al. 3.
16. Art. 15, § 2, al. 5.
17. L'appel aux candidatures mentionne néanmoins que « *quoiqu'il n'y ait pas d'exigence légale concernant les membres, constitue un atout pour les candidats une connaissance dans un ou plusieurs des domaines suivants :*
– la connaissance du droit de l'informatique,
– la connaissance et la gestion du fonctionnement des réseaux informatiques,
– des capacités de gestion et d'organisation,
– la connaissance du droit judiciaire » (*M.B.*, 19 septembre 2005, 2e éd., pp. 40510 et s.)

Enfin, le comité doit être paritaire d'un point de vue linguistique [18] et tenir compte d'une participation la plus équilibrée possible sur le plan fonctionnel et de la parité homme/femme [19].

9 Le comité de gestion a une compétence de décision, de proposition et d'avis.

1. *Une compétence de décision*

« Le comité de gestion gère Phenix et prend toute initiative qui peut améliorer son efficacité, en conformité avec les dispositions de la présente loi, du Code judiciaire, du Code d'instruction criminelle et les autres dispositions légales pertinentes. Il prend toutes les décisions requises par la présente loi » [20].

En particulier, il décide de :

- la conclusion des accords techniques relatifs à la gestion du système,
- l'adoption des codes,
- la certification de la conformité des documents électroniques issus de la conversion des documents papiers ou des documents électroniques qui doivent migrer vers un autre format,
- l'adaptation du système aux modifications législatives, réglementaires ou technologiques, notamment en matière de simplification du langage judiciaire [21].

Il définit les mécanismes de contrôle :

- à l'entrée des installations où sont localisés les traitements de données,
- de mémoire des ordinateurs traitant de données,
- des supports sur lesquels les données sont stockées,
- de l'introduction des données,
- de disponibilité des traitements de données,

18. Art. 15, § 5. Voy. aussi l'art. 15, § 2, al. 4 qui impose que le président et le vice-président soient de rôle linguistique différent.
19. Art. 15, § 3.
20. Art. 17, al. 1.
21. Art. 17, al. 7 et s.

- de l'utilisation des traitements de données,
- de la communication des données,
- d'accès aux traitements de données,
- de mécanisme d'archivage des données,
- du choix des standards techniques utilisés pour la sauvegarde et la communication des données [22].

2. *Une compétence de proposition*

10 La loi Phenix et le projet de loi relative à la procédure par voie électronique [23] octroient un large pouvoir de proposition au comité de gestion : pour les principales modalités d'exécution des différentes finalités de Phenix, ainsi que pour un certain nombre de dispositions du projet de loi relative à la procédure électronique, le Roi prend ses arrêtés sur proposition du comité de gestion et après avoir entendu l'avis du comité de surveillance [24].

Ce pouvoir de proposition signifie que le comité de gestion a un pouvoir d'initiative et qu'il détermine le calendrier des travaux réglementaires relatifs à Phenix.

Certes, l'article 29 de la loi Phenix dispose que « *le comité de gestion, saisi par le Ministre d'une demande de proposition ou d'avis relative à un arrêté formule la proposition dans les trente jours de la demande* ». Ce faisant, la loi donne un pouvoir d'initiative au ministre de la Justice, mais celui-ci doit néanmoins rester l'exception, sous peine de réduire à néant les compétences du comité de gestion, dont la composition paritaire concrétise l'équilibre entre le pouvoir judiciaire et exécutif.

3. *Une compétence d'avis*

11 Le comité de gestion a une compétence d'avis à l'égard des acteurs principaux de Phenix, à savoir le ministre de la Justice et la Cour de cassation.

22. Art. 19. Ces mesures de sécurité constituent le standard en matière de sécurité de banques de données (art. 118 de la convention d'application de Schengen, art. 22 du règlement n° 45/2001 du Parlement européen et du conseil, art. 25.2 de la convention Europol, etc.).
23. *Doc. parl.*, Ch., 2005-2005, 1701/001.
24. Pour la liste des arrêtés royaux, *cfr. infra*, n[os] 22 et s.

Chaque année il leur remet un rapport annuel sur l'activité de Phenix, en ce compris les prévisions budgétaires [25]. En outre, il leur remet des avis ponctuels, d'initiative ou suite à la constatation d'anomalies ou de manquements aux règles de Phenix [26].

12 À propos des **recours** contre les décisions du comité de gestion, la Cour de cassation, suivant l'article 610 modifié du Code judiciaire est compétente pour connaître des demandes en annulation des actes du comité de gestion qui excéderaient ses pouvoirs, seraient contraires aux lois ou pris de manière irrégulière [27]. Cette compétence est sans préjudice de la compétence du président du tribunal de première instance statuant comme en référé [28], telle que prévue par l'article 14 de la loi du 8 décembre 1992.

B. Le comité de surveillance

13 À côté du comité de gestion, chargé de la gestion quotidienne de Phenix, est institué un comité de surveillance, chargé du contrôle du respect des règles de la loi du 8 décembre 1992 appliquées à Phenix.

À l'instar des autres banques de données de l'État (Registre national des personnes physiques, banque-carrefour de la sécurité sociale, banque-carrefour des entreprises), le comité de surveillance constitue, conformément à l'article 31*bis* de la loi du 8 décembre 1992, un comité sectoriel institué au sein de la C.P.V.P. [29].

25. Art. 21.
26. Art. 20.
27. Loi du 10 août 2005 modifiant l'article 610 du Code judiciaire, *M.B.*, 1[er] septembre 2005, p. 38312.
28. *Doc. parl.*, Ch., 1646/001, p. 27. Nous reviendrons *infra*, n° 59 sur le problème posé par ce renvoi.
29. Sur les comités sectoriels institués au sein de la Commission de la protection de la vie privée, cfr. loi du 26 février 2003 modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une banque-carrefour de la sécurité sociale en vue d'aménager et d'étendre les compétences de la commission de la protection de la vie privée, *M.B.*, 26 juin 2003 ; A.R. du 17 décembre 2003 fixant les modalités relatives à la composition et au fonctionnement de certains comités sectoriels au sein de la Commission de la protection de la vie privée, *M.B.*, 30 décembre 2003.

Le projet de loi initial prévoyait un comité de surveillance, indépendant de la Commission de la protection de la vie privée, composé exclusivement de magistrats de l'Ordre judiciaire avec la présence, avec voix consultative, d'un représentant de la Commission et donnait compétence à la Cour de cassation d'annuler les actes du comité de surveillance qui seraient entachés d'excès de pouvoir [30].

Dans son avis, la Commission de la protection de la vie privée a souhaité que le comité de surveillance soit inséré au sein de la Commission vie privée, qu'il soit composé de trois membres externes et de trois membres désignés par la Commission vie privée en son sein, dont le président, que la Commission puisse évoquer les décisions du comité sectoriel et qu'en cas de parité de vote, la voix du président soit prépondérante [31].

14 Le législateur s'est majoritairement rangé à l'avis de la Commission de la protection de la vie privée : le comité de surveillance Phenix est institué au sein de la Commission de la protection de la vie privée et composé de trois membres désignés au sein de la Commission de la protection de la vie privée et de trois membres externes désignés, tout comme pour les autres comités sectoriels, par la Chambre, sur proposition du Conseil des ministres [32].

Ce comité est néanmoins particulier en ce que les membres externes doivent être des magistrats de l'Ordre judiciaire et qu'ils sont désignés après avis conforme et conjoint du premier président et du procureur général près la Cour de cassation [33].

Autre différence également, la présidence, assurée dans les autres comités sectoriels par le président de la Commission de la protection de la vie privée, est assurée par un des membres externes.

30. *Doc. parl.*, Ch., 2004-2005, p. 89.

31. Cf. avis 11/2004 de la Commission de la protection de la vie privée, point 22, *in Doc. parl.*, Ch., 2004-2005, 1645/001, p. 91.

32. Art. 22.

33. À noter la différence de procédure d'avec le comité de gestion, où certains membres sont proposés par la Cour de cassation au Conseil de ministre. Pour le comité de surveillance, le Conseil des ministres élabore une première liste qui est ensuite soumise à l'avis de la Cour de cassation. Le pouvoir d'initiative change donc mais est tempéré par le fait que l'avis de la Cour de cassation doit être conforme.

Le législateur a estimé nécessaire qu'un magistrat de l'Ordre judiciaire préside le comité de surveillance de Phenix. Or, la loi vie privée ne contient aucune obligation que des magistrats de l'Ordre judiciaire siègent au sein de la Commission vie privée. Elle prévoit uniquement que des magistrats doivent y siéger [34], cette qualité ne visant pas uniquement celle de magistrat de l'Ordre judiciaire mais englobant également les auditeurs et référendaires au Conseil d'État ou à la Cour d'arbitrage [35].

En outre, le législateur a estimé que « l'attribution de la présidence à un membre proposé par la Cour de cassation permet de respecter et de concrétiser de manière plus adéquate le principe de la séparation des pouvoirs » [36].

15 Quant aux **compétences** du comité de surveillance, l'équilibre à trouver ici est celui entre l'indépendance constitutionnelle du pouvoir judiciaire et l'indépendance légale de la Commission de la protection de la vie privée, et doit garantir que chacun puisse poursuivre les objectifs que la loi ou la Constitution lui attribue.

Le comité de surveillance de Phenix connaît dès lors des **plaintes** relatives à l'application de la loi vie privée au système Phenix [37]. Lorsqu'il constate une infraction à la loi, il la dénonce au parquet [38].

Ces plaintes peuvent émaner d'un justiciable à l'encontre d'un juge d'instruction, d'un juge à l'égard de son chef de corps, d'un avocat à l'encontre du comité de gestion, etc.

Cette compétence de connaître des plaintes est limitée dans son champ d'application : le comité de surveillance n'a de compétence que pour contrôler le respect de l'application de la loi du 8 décembre 1992 relative à la protection de la vie privée à la banque de données Phenix [39], la Commis-

34. Ces magistrats ne semblent pas faciles à trouver après trois appels à candidatures parus au *Moniteur belge*.

35. *Doc. parl.*, Ch., 2001-2002, 1940/001, pp. 10-11.

36. *Doc. parl.*, Ch., 1645/001, p. 20.

37. Art. 24 § 1er, al. 2 et 3.

38. Art. 24, § 3.

39. Art. 24, § 1er, al. 2.

sion vie privée elle-même étant compétente pour connaître des plaintes relatives aux autres domaines de la protection de la vie privée [40].

Cette compétence est également limitée dans son effet : le traitement des plaintes ne peut déboucher que sur un avis, un procès verbal de conciliation, voire une transmission du dossier au parquet [41].

Il appartiendra aux cours et tribunaux d'apprécier la question de savoir si l'illégalité commise ne compromet pas un procès équitable et n'entache pas la fiabilité de la preuve [42].

16 Outre cette première compétence, le comité de surveillance dispose d'une compétence d'**avis** générale sur toute question relative à l'application de la loi du 8 décembre 1992 à Phenix. Ainsi il pourra se prononcer sur l'application des principes de légitimité (voir *infra*, n° 32) et sur les modalités d'application des droits subjectifs des personnes concernées (voir *infra*, n° 53).

17 Contrairement aux autres comités sectoriels institués au sein de la Commission de la protection de la vie privée [43], le comité de surveillance de Phenix n'a pas de pouvoir de délivrer l'accès aux données. L'accès aux données du dossier judiciaire est en effet régi, selon l'exposé des motifs, par les dispositions du Code judiciaire ou du Code d'instruction criminelle.

Il n'a pas non plus comme le comité « registre national » ou le comité de surveillance des banques carrefour sécurité sociale ou entreprises, le pouvoir d'autoriser ou d'interdire des communications au sein de Phenix, celles-

40. *Doc. parl.*, Ch., 1645/001, p. 22.

41. *Id.*

42. Cass., 14 octobre 2003, cité par J. Leclerq et D. De Roy, « La jurisprudence de la Cour de cassation en matière de la vie privée dans le cadre des relations de travail », in *Vie privée des travailleurs et prérogatives patronales*, Bruxelles, éd. du jeune barreau de Bxl, 2005.

43. L'article 31*bis* de la loi de 1992, tel qu'introduit par la loi du 26 février 2003, institue la possibilité de création, au sein de la Commission de protection de la vie privée, de comités sectoriels compétents pour instruire et statuer à propos de demandes relatives aux traitements où aux communications de données faisant l'objet de législations particulières. Ainsi, sur le modèle du comité de surveillance de la Banque-Carrefour de la sécurité sociale, ont été créés les comités sectoriels du registre national, de la Banque Carrefour des entreprises, de l'autorité fédérale.

ci étant également régies, toujours selon l'exposé des motifs, par les dispositions du Code judiciaire ou du Code d'instruction criminelle [44].

18 Le problème des questions préjudicielles susceptibles d'être posées à la Commission de la protection de la vie privée a fait l'objet d'un débat difficile. L'article 31*bis*, § 3, alinéa 3, dernière phrase de la loi du 8 décembre 1992 dispose que, « *sans préjudice de l'article 44 de la loi du 15 janvier 1990 relative à l'institution et l'organisation d'une banque-carrefour de la sécurité sociale, le Président du comité sectoriel peut décider de suspendre l'examen d'un dossier afin de le soumettre à la Commission (de la protection de la vie privée) qui rend sa décision dans un délai d'un mois* ».

À l'origine, le projet de loi n'avait pas prévu de possibilité pour la Commission vie privée de connaître des avis du comité de surveillance de Phenix, d'une part parce que contrairement aux autres comités sectoriels, le comité de surveillance de Phenix n'a pas de pouvoir de décision, exception faite de celle de transmettre un dossier au parquet. « *Par ailleurs, autoriser la Commission de la protection de la vie privée à évoquer des avis du comité de surveillance de phenix serait remettre en cause l'équilibre des pouvoirs entre la Commission de la protection de la vie privée et l'Ordre judiciaire, tous deux constitutionnellement ou légalement indépendants* » [45].

La Commission vie privée avait néanmoins estimé essentiel de pouvoir évoquer les décisions du comité de surveillance de Phenix [46] et le Conseil d'État avait suivi partiellement l'avis de la Commission, en demandant à ce

44. *Doc. parl*, Ch., 1645/001, p. 23. Ces assertions de l'exposé des motifs tant sur l'accès aux dossiers judiciaires que sur l'accès aux banques de données externes semblent un peu légères. Certes, certaines dispositions évoquent le droit des justiciables à accéder à leurs propres dossiers mais quid du droit d'un témoin ou d'une personne citée ? Quid surtout du droit d'autres membres du pouvoir judiciaire à accéder à des dossiers relatifs à des personnes citées devant eux ? En ce qui concerne l'accès aux banques externes, les autorisations prévues par les lois gouvernant ces banques de données ne sont-elles pas d'application ? Sur ces points, nos réflexions à propos du droit d'accès, *infra*, n^{os} 58 et s., sur les droits d'utilisation des banques de données externes, *infra*, n° 42.

45. *Doc. parl*, Ch., 2004-2005, 1654/001, p. 42.

46. Cf. avis n ° 11/2004 de la Commission de la protection de la vie privée, point 22, *in Doc. parl.*, Ch., 2004-2005, 1645/001, p. 91. « *L'argument pris du respect de la séparation des pouvoirs et de l'indépendance du pouvoir judiciaire - éminemment respectable en soi - appelle toutefois, utilisé dans le contexte du présent dossier, plusieurs observations.*

que l'on veille à une meilleure articulation entre les deux organes, « *à défaut de quoi, l'intégration du comité de surveillance spécialisé dans le cadre général de la loi du 8 décembre 1992 paraîtra artificelle* » [47].

Dès lors, la loi Phenix dispose, à l'instar des autres comités sectoriels institués au sein de la Commission de la protection de la vie privée, que l'examen d'un dossier soumis au comité de surveillance est suspendu à la demande de deux membres du comité de surveillance de Phenix afin de le soumettre au préalable à la Commission de la protection de la vie privée [48].

Néanmoins, afin de respecter le principe d'indépendance du pouvoir judiciaire, la loi Phenix, s'inspirant du précédent de la banque-carrefour de

a) Tout d'abord, comme les autres pouvoirs constitués, le pouvoir judiciaire est soumis au titre II de la Constitution « Des Belges et de leurs droits », et notamment à l'article 22 de celle-ci qui garantit le droit au respect de la vie privée. Il importe dès lors que, également en ce qui concerne le traitement des données judiciaires, cette liberté fondamentale soit respectée et ce, en outre, sans qu'il n'y ait de discrimination dans le bénéfice de cette liberté publique — conformément au prescrit des articles 10 et 11 de la Constitution.

b) La Commission observe ensuite que la nécessité que la protection de la vie privée soit dûment assurée en la présente matière, notamment sur le plan institutionnel, s'impose d'autant plus que sont en cause des données sensibles — les données judiciaires — pour lesquelles, dès l'origine, la loi du 8 décembre 1992 a prévu un régime de protection renforcé ; celui-ci est actuellement fixé à l'article 8 de la loi précitée et à l'article 25 de l'arrêté royal du 13 février 2001. L'affaiblissement global du degré de protection, comparativement aux autres domaines déjà réglementés sur ce plan par le législateur, auquel conduirait le Comité de surveillance dans la conception retenue par le projet, va à l'encontre du régime renforcé que commande, au contraire, la réglementation de données judiciaires.

c) Il peut être également relevé, malgré le respect que requiert le principe de l'indépendance judiciaire, que celui-ci n'implique pas - dans notre système juridique - que tous les actes, qui de façon plus ou moins directe le concernent, doivent nécessairement être examinés par des organes composés exclusivement de magistrats judiciaires. Ainsi peut-on relever que des organes aussi différents que le Conseil supérieur de la Justice, le Conseil d'État, la Cour d'arbitrage ou la Cour des comptes sont-ils amenés, chacun dans le cadre de leur compétence, à poser des actes qui ne sont, manifestement, pas sans incidence sur le fonctionnement du pouvoir judiciaire, qu'il s'agisse de ses membres, de ses compétences ou de son organisation.

d) Enfin, la Commission observe que le Comité de gestion, dans l'approche même du projet, ne doit pas être magistrat (cf. art. 5 et 6), nonobstant le rôle important de cet organe dans le cadre du projet Phenix ».

47. *Id.*, p. 43.

48. Art. 24, § 2.

la sécurité sociale [49], n'instaure pas de préséance entre l'avis rendu par la Commission de la protection de la vie privée et celui rendu par le comité de surveillance de Phenix : si les deux organes ne parviennent pas à s'entendre, le comité de surveillance motive explicitement les raisons pour lesquelles le point de vue de la Commission vie privée n'a pas du tout ou a été partiellement suivi et les deux avis sont communiqués [50].

C. Le comité d'utilisateurs

19 La loi Phenix institue « *un comité d'utilisateurs, chargé de proposer au comité de gestion toute initiative de nature à promouvoir l'utilisation de Phenix* » [51]. On regrette avec la Commission de protection de la vie privée qu'il (ou certains de ses membres) n'ait point reçu la possibilité de saisir le Comité de surveillance [52].

Ce comité d'utilisateurs est composé de 24 membres dont 16 membres de l'Ordre judiciaire et 8 représentants des auxiliaires de justice (4 avocats, 2 huissiers de justice, 2 notaires).

Pour être plus précis, on épingle comme membres de ce comité :

- 2 représentants désignés par la Cour de cassation, l'un appartenant au siège, l'autre appartenant au parquet de la Cour,
- 2 représentants désignés par les premiers présidents des cours d'appel et du travail,
- 2 représentants désignés par le collège des procureurs-généraux,
- 2 représentants désignés par le Conseil des procureurs du Roi,

49. *Cf. art. 44 de la loi du 15 janvier 1990 relative à l'institution et l'organisation d'une banque-carrefour de la sécurité sociale, qui supprime également la préséance de l'avis de la Commission de la protection de la vie privée sur celui du comité sectoriel de la sécurité sociale.*

50. Art. 24, § 2.

51. Art. 27, al. 1.

52. Avis n° 11/2004 : « *L'ouverture du comité n'oblige-t-elle pas accueillir d'autres demandes d'avis, ainsi celles en provenance des avocats ou d'autres représentants des justiciables et le devoir de transparence ne conduit-il pas à une meilleure diffusion des décisions et des rapports y produits ? À cet égard, les rapports entre le comité d'utilisateurs visé à l'article 18 et le comité de surveillance devraient être mieux définis. Un droit de saisir le comité de surveillance devrait exister pour les différentes catégories "d'utilisateurs"* ».

- 2 représentants désignés par le Conseil des auditeurs du travail,
- 2 représentants désignés par le Conseil supérieur de la Justice,
- 2 représentants désigné par l'Orde van de Vlaamse balies,
- 2 représentants désignés par l'Ordre des barreaux francophone et germanophone,
- 2 représentants désignés par la Chambre nationale des huissiers de Justice,
- 2 représentants désignés par la Fédération royale du notariat belge,
- 2 représentants du personnel des secrétariats des parquets et des auditorats désignés par le ministre de la Justice,
- 2 représentants du personnel des greffes désignés par le ministre de la Justice.

Il désigne en son sein un président et un vice-président, dont l'un des deux au moins doit être un auxiliaire de justice [53].

20 Le comité des utilisateurs est chargé de faire des propositions au comité de gestion de Phenix, qui est légalement tenu de les examiner et d'y répondre de manière motivée [54].

Le président et le vice-président du comité des utilisateurs siègent également au sein du comité de gestion avec voix consultative [55].

53. Art. 27, al. 6.

54. Art. 17, al. 6. Sur ce point, on note que le texte de la loi a suivi l'avis de la Commission de la protection de la vie privée : « *À cet égard, il est intéressant de noter que le Conseil supérieur de la Justice (C.S.J., Avis rectificatif au projet de loi instituant la banque de données Phenix, approuvé par l'Assemblée générale, le 26 mai 2004) avait souhaité pour la même raison un fonctionnement plus ouvert du comité et réclame de pouvoir solliciter l'avis du Comité de surveillance et de bénéficier d'une copie du rapport d'activités.*
L'ouverture du comité n'oblige-t-elle pas accueillir d'autres demandes d'avis, ainsi celles en provenance des avocats ou d'autres représentants des justiciables et le devoir de transparence ne conduit-il pas à une meilleure diffusion des décisions et des rapports y produits ? À cet égard, les rapports entre le Comité d'utilisateurs visé à l'article 18 le comité de surveillance devraient être mieux définis. Un droit de saisir le comité de surveillance devrait exister pour les différentes catégories "d'utilisateurs" ».

55. Art. 15, § 7. Sans doute, eût-il été plus judicieux d'accorder à ces représentants du comité d'utilisateurs une voix plus importante.

D. Le Roi

21 À côté des organes de Phenix proprement dit, il faut également mentionner le rôle du Roi : les deux lois Phenix ne requièrent pas moins de quarante mesures d'exécution dont 29 arrêtés royaux.

Pour la loi du 10 août 2005, le Roi détermine, sur proposition du comité de gestion et après avis du comité de surveillance,

- concernant la gestion et la conservation des dossiers judiciaires, les règles d'accès et d'authentification d'accès [56],
- concernant le rôle national, les règles d'accès et d'authentification d'accès [57],
- concernant la banque de données de jurisprudence interne, les modalités d'accès, des catégories des personnes ayant accès et les mesures de sécurité particulières [58],
- concernant la banque de données de jurisprudence externe, des modalités d'anonymisation des décisions et des exceptions au principe d'anonymisation [59],
- concernant l'élaboration de statistiques externes, des règles d'anonymisation ou de codification des données nécessaires à leur élaboration [60],
- concernant l'élaboration de statistiques internes et externes, des modalités d'exécution [61].

22 Pour la future loi relative à la procédure électronique, il s'agit de :

- l'article 4, où le Roi, après avis du comité de gestion, peut :
  1° disposer que certaines catégories de personnes physiques ou morales sont tenues de poser des actes de procédure par voie électronique,

56. Art. 5.
57. Art. 6.
58. Art. 8.
59. Art. 9.
60. Art. 12.
61. Art. 13.

2° abroger des dispositions légales afin de permettre la communication par voie électronique entre sujets de droits et autorités judiciaires,

3° fixer les modalités selon lesquelles les citoyens peuvent communiquer avec les autorités judiciaires ;

- l'article 8 où le Roi fixe, après avis du comité de gestion, les modalités et les formes des paiements lors des dépôts, remises ou prise de connaissance des pièces de procédure par voie électronique ;
- Les articles 2, 4° et 10 où le Roi détermine, après avis du comité de gestion et après avis du comité de surveillance, les conditions d'application des exigences mises à charge des prestataires de services de communication ;
- l'article 16 où le Roi détermine, après avis du comité de gestion, les formes selon lesquelles l'accord, la renonciation ou la modification de l'adresse judiciaire électronique doit être donné ;
- les articles 21 à 25 et 53 où le Roi détermine, après avis du comité de gestion et du comité de surveillance, les modalités de création, de conservation et de communication des registres et des répertoires ;
- l'article 28 où le Roi détermine, après avis du comité de gestion et du comité de surveillance, les modalités de création et de conservation du rôle ;
- les articles 49, § 3 et 51, § 2 où le Roi détermine, sur proposition du comité de gestion, les modalités d'introduction de la signature électronique qualifiée en matière pénale.
- l'article 52, § 1er où le Roi fixe, après avis du comité de gestion, la date de l'introduction complète du dossier électronique en matière pénale.

23 On pourrait s'étonner du rôle donné à l'exécutif pour un système destiné en premier lieu à l'Ordre judiciaire. La Commission justice du Sénat s'était d'ailleurs émue des nombreuses délégations au Roi accordées par la loi du 10 août 2005, se demandant si elles étaient compatibles avec la convention n° 108 du Conseil de l'Europe [62].

Le fait est que les lois Phenix sont des lois expérimentales et intimement liées au système informatique Phenix lui-même. Il n'était dès lors pas

62 *Doc. parl.*, Sén., Sess. 2004-2005, 3-1163, pp. 11 et s

possible de mettre certaines mesures pratiques dans la loi elle-même dans l'ignorance du contenu de ces mesures d'exécution et sauf à devoir modifier sans cesse les lois en fonction de l'évolution technologique.

La solution initialement retenue avait été de confier au comité de gestion la compétence de décider seul des mesures d'exécution, mais la Commission vie privée l'avait écartée en disant que « *pour fixer la répartition des rôles dans le respect des règles de droit (...), la loi devrait énoncer les finalités déterminées (...). Sur cette base légale au sens strict et formel, un arrêté royal pris après avis de la Commission et délibéré en Conseil des ministres devrait fixer les règles de base des différents traitements de données, à savoir les types de données traitées et les catégories des utilisateurs, laissant ensuite au comité de surveillance de détailler celles-ci et ceux-ci sur base des principes de proportionnalité et de sécurité (...) Cette répartition des tâches entre loi, arrêté royal délibéré en Conseil des ministres sur avis de la Commission, comité de surveillance et comité de gestion est essentielle afin de garantir à la fois, dans le respect de l'article 22 de la Constitution, la protection de la vie privée et le respect des principes constitutionnels de répartition des compétences entre les trois pouvoirs* » [63]. La loi a suivi ce point de vue.

24 D'aucuns pourraient s'inquiéter de ce qu'ils pourraient considérer comme une trop grande main-mise de l'exécutif sur une banque de données judiciaires. Mais la loi ne délègue au Roi la compétence de prendre des mesures que sur le fonctionnement et la structure du système d'information Phenix : il n'a aucun pouvoir sur la fonction juridictionnelle même ni le contenu des dossiers.

E. Le S.P.F. Justice

25 La loi octroie au S.P.F. Justice deux missions : d'une part, il inscrit à son budget les crédits nécessaires à la création et, au fonctionnement de Phenix [64], ainsi que les frais de fonctionnement des comités de gestion et des utilisateurs [65]. D'autre part, il appuie le comité de gestion pour l'exécution de sa mission [66].

63. *Doc. parl.*, Ch., 1645/001, pp. 84 et s.
64. Art. 2, al. 3.
65. Art. 28, al. 1.
66. Art. 28, al. 2.

F. Conclusion sur l'équilibre de pouvoirs au sein de Phenix

26 La composition, la désignation et le mode de fonctionnement des différents comités tentent d'établir un équilibre entre les pouvoirs exécutif, judiciaire et législatif.

Les solutions initialement prévues étaient davantage centrées sur l'Ordre judiciaire, en instituant un comité de gestion avec plus de pouvoirs et un comité de surveillance indépendant de la Commission de la protection de la vie privée, composé uniquement de membres de l'Ordre judiciaire.

Suite aux avis de la Commission de la protection de la vie privée et du Conseil d'État,

- les finalités du système ont été précisées davantage dans la loi [67],
- le Roi s'est vu confié certaines tâches initialement confiées au comité de gestion,
- le Comité de surveillance a été intégré dans la Commission de la protection de la vie privée.

Il en résulte une procédure extrêmement complexe, qui, espérons-le, garantit le respect de l'indépendance des pouvoirs, tout en ne bloquant pas le fonctionnement et le développement de Phenix, tout en garantissant le respect des principes de la loi de 1992.

67. Cf. *infra*, section 2, n° 38 à propos des communications internes et externes ; n^{os} 48 et s. à propos des banques de données jurisprudentielles ; n° 51 à propos de l'aide à la gestion.

SECTION 2

De l'examen des finalités de Phenix et d'autres considérations relatives à l'application de la loi du 8 décembre 1992

27 L'introduction rappelait le contenu de l'article 2 de la loi Phenix qui énumère les diverses finalités de ce système d'informations. Cette énumération conduit à rappeler, dans un premier temps, la signification concrète du principe de « finalité » qui fixe les conditions de légitimité de l'existence d'un traitement et d'autres principes directement liés à celui-ci visant cette fois le contenu des traitements opérés dans le cadre des finalités. Au-delà de l'analyse des finalités prévues par la loi Phenix, on s'interroge : la liste des finalités prévues par le texte de la loi Phenix est-elle complète ? Pour répondre à cette interrogation, il sera nécessaire d'envisager non seulement les prescrits de la loi Phenix mais au-delà de considérer le second volet légal du projet Phenix, à savoir le projet de loi relatif à la procédure par voie électronique toujours en discussion à l'heure actuelle [68].

Dans un second temps, on abordera les autres conséquences de l'application de la loi du 8 décembre 1992. Ainsi, cette loi accorde aux personnes concernées quelques droits dont l'exercice devra tenir compte de règles fondamentales du fonctionnement de la Justice ; elle soumet le responsable du traitement à des obligations, en particulier celle de sécurité et prévoit des recours en cas de violation de ses prescrits.

68. Projet de loi relatif à la procédure par voie électronique, *Doc. parl.*, Ch. Repr. 1701/001 Session 2004-2005.

A. Les finalités de Phenix

1. *Rappel du principe de finalité et des principes accessoires à celui-ci*

28 L'article 4 est sans doute l'article le plus fondamental de la législation dite « Vie privée » [69]. Il énonce :

« Les données à caractère personnel doivent être :

1° traitées loyalement et licitement ;

2° collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible lorsqu'il est effectué conformément aux conditions fixées par le Roi, après avis de la Commission de la protection de la vie privée ;

3° adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement ;

4° exactes et, si nécessaires, mises à jour ; toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées ;

5° conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement. Le Roi prévoit, après avis de la Commission de la protection de la vie privée, des garanties appropriées pour les données à caractère personnel qui sont conservées au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques ».

En d'autres termes, l'article établit nombre de principes articulés autour de la question de la légitimité des traitements. La loyauté, la nécessité

69. Voy. T. Leonard, Y. Poullet, « Les libertés comme fondement de la protection des données nominatives », in F. Rigaux, *La vie privé, une liberté parmi les autres ?*, Travaux de la Faculté de droit de Namur, n° 17, Bruxelles, larcier, pp. 231 et s. ; S. Gutwirth, « De toepassing van het finaliteitbeginssel van de privacywet van 8 december 1992 tot bescherming van de persoonlijke levensfeer ten opzicht van de verwerking van persoonsgegevens », *T.P.R.*, 1994, pp. 1409-1477.

de finalités déterminées, explicites et légitimes, la non utilisation des données de manière incompatible avec les finalités de la collecte, la restriction du contenu des traitements à des données adéquates nécessaires et pertinentes au regard des finalités poursuivies, l'exigence de qualité est finalement la limitation de la conservation dans le temps.

Chacun de ces principes fait l'objet de quelques développements [70]. On notera à cet égard l'apport de la jurisprudence de la Cour d'arbitrage.

29 **La loyauté** d'un traitement exige que celui-ci soit « prévisible » par la personne concernée. L'exigence fait référence aux conditions de prévisibilité et d'accessibilité de la loi posées par la jurisprudence découlant de l'article 8.2 de la Convention européenne des droits de l'homme lorsqu'elle autorise l'autorité publique à s'ingérer dans la vie privée des citoyens. Comme le note le Conseil d'État belge, à propos d'une décision concernant la sûreté de l'État [71] : « *Considérant que l'article 8, § 2 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales permet l'ingérence de l'autorité publique dans l'exercice du droit de toute personne au respect de la vie privée, pour autant que cette ingérence est conforme à la loi, qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire notamment à la sécurité nationale et à la sûreté publique, et que les textes qui la prévoient soient accessibles à l'intéressé et rédigés en termes assez clairs pour lui indiquer de manière adéquate quelles circonstances et sous quelles conditions, ils habilitent la puissance publique à s'y livrer, spécialement si l'ingérence présente un caractère secret* » [72].

30 L'exigence du **caractère déterminé et explicite des finalités** d'un traitement proscrit toute imprécision dans l'expression des finalités poursuivies.

70. Pour une application de ces principes aux traitements opérés par un cabinet d'avocats, lire C. de Terwangne, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », in *Cabinets d'avocats et technologies de l'information*, J.F. Henrotte — Y. Poullet (éd.), Cahiers du C.R.I.D., n° 26, Bruylant, 2005, pp. 156 et s.

71. Sur le rôle joué par la jurisprudence du Conseil d'État dans l'adoption de la loi organique du 30 nov. 1998 des services de renseignements et de sécurité (*M.B.*, 18 décembre 1998), voy. B. Havelange, Y. Poullet, « Secret d'État et vie privée ou comment concilier l'inconciliable », in *Droit des Technologies de l'Information — Regards prospectifs*, E. Montero (éd), Cahier du C.R.I.D., n° 16, Bruxelles, Bruylant, 1996.

72. Arrêt Wicart, C.E., 30 juin 1995, Arrêt n° 54-139.

La finalité doit être énoncée en termes clairs, complets et précis. Si un système d'information poursuit diverses finalités, le responsable du traitement veillera à la transparence de chacun des traitements, de manière à ce que « *la personne concernée puisse raisonnablement, à l'énoncé de la lecture de chaque finalité, concevoir les types d'applications couverts par cette finalité* » [73]. Il s'agit de permettre ainsi le contrôle de la légitimité du traitement tant par personne concernée que par toute personne qui, notamment via le registre public, prendra connaissance des traitements poursuivis par une entreprise ou une administration.

> « Un double régime s'instaure donc concernant la poursuite de telles finalités. Si la finalité initiale annoncée est une finalité historique, statistique ou scientifique, le traitement reste soumis aux seules règles légales commentées. Si, par contre, la finalité annoncée lors de la collecte était différente et incompatible avec de telles finalités — par exemple, l'exécution d'un contrat de prestation de services — et qu'ultérieurement le responsable du traitement veut utiliser ces données en vue de réaliser, par exemple, une étude statistique de marché, il doit se conformer au régime complexe organisé par les articles 2 à 24 de l'arrêté royal.
>
> Retenons seulement ici que le principe de base de cet arrêté [74] est qu'il incombe au responsable du traitement de ne travailler qu'avec des données anonymes. Si cela s'avère impossible, il doit alors coder les données et se soumettre aux règles particulières propres aux traitements de telles données. Si un tel codage est impossible, il doit se soumettre au régime spécifique au traitement de donnes non codées. Les conditions de traitement sont à chaque étape de plus en plus strictes : de l'absence de protection pour les données anonymes à un régime de consentement préalable pour les données non codées » [75].

73. J.P. Buyle, L. Lannoye, Y. Poullet, V. Willems, « Le droit de l'informatique, Chronique de jurisprudence (1987-1994) », *J.T.*, 1996, p. 233, n° 65, *in fine* à propos de l'affaire KB Bancassurance (Comm. Anvers (Prés.) 7 juillet 1994, *Computerrecht*, 1994, pp. 244 et s., note J. Dumortier et F. Robben, *DIT*, 1995, p. 55, note O. Lesuisse).

74. Sur cet arrêté, lire I. Anne, « De verwerking van persoonsgegevens voor wetenschappelijk onderzoek », *Computerrecht*, 2000, pp. 288 à 296 ; D. De Bot, « Verwerking van persoonsgegevens », *op. cit.*, pp. 101 à 110 ; C. de Terwangne et S. Louveaux, « La protection de la vie privée face au traitement de données à caractère personnel : le nouvel arrêté royal », *J.T.*, 2001, pp. 465 à 469.

75. T. Leonard, « La protection des données à caractère personnel et l'entreprise », in *Guide juridique de l'entreprise*, 2e éd., Titre XI, Livre 112, Diegem, Kluwer, 1996, pp. 23 et s.

51 La **légitimité d'un traitement** s'entend de son caractère nécessaire et de sa proportionnalité à l'objectif poursuivi par celui-ci.

Ainsi, la légalité d'un traitement ne dispense pas d'autres examens, ceux de légitimité et de proportionnalité. Un traitement dans l'administration non seulement doit disposer d'une base légale mais en outre doit être conforme au but poursuivi par cette loi et ne pas être disproportionné à celui-ci [76]. C'est l'enseignement majeur d'une décision de la Cour d'arbitrage du 18 février 1993 [77]. En l'occurrence, il s'agissait de savoir si la communication par écrit à la commune du nom des ménages qui ont fait l'objet d'un placement d'un limitateur de consommation électrique, portait atteinte à la vie privée des personnes concernées. La Cour estime, après avoir noté qu'une telle information est bien relative à la vie privée du ménage,

- que « *parmi les droits et libertés garantis par les articles 6 et 6bis de la Constitution figurent bien les droits et libertés résultant de dispositions conventionnelles internationales liant la Belgique et rendues applicables dans l'Ordre juridique interne par un acte d'assentiment. Il en est ainsi à tout le moins des droits et libertés résultant de dispositions ayant effet direct, ce qui est le cas de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et de l'article 17 du Pacte international du 19 décembre 1966 relatif aux droits civils et politiques* » ;
- que « *toutefois, cette ingérence dans la vie privée est prévue par une loi au sens de l'article de la Convention européenne. Elle n'est qu'une modalité d'un ensemble de mesures qui, en interdisant les coupures de courant, visent à protéger la santé d'une catégorie de personnes.*

76. *Cfr*, à ce propos, la décision du tribunal de commerce de Bruxelles du 20 mars 1995 qui précise les finalités du registre des immatriculations automobiles : « *Selon le tribunal, la légalité n'est pas respectée lorsqu'un traitement, en l'espèce la communication des fichiers de l'administration des transports, à un opérateur économique, est décidée par le ministre, sans délégation de compétences par la loi. Quant à la proportionnalité, elle n'existe pas à défaut d'existence d'un problème précis de sécurité risquant d'affecter les véhicules de la marque. Les exigences de sécurité qui légitimeraient l'utilisation par Mercedes d'un tel traitement ne peuvent justifier ce qui, de toute évidence, constitue une opération de marketing* » (voir J.-P. Buyle, V. Willems, Y. Poullet, « Le droit de l'informatique : chronique de jurisprudence », *JT*, 1996, p. 232).

77. C.A., arrêt 14/93, 18 février 1993, Arrêt C.A., 1993, pp. 153 et s. ; *R.W.*, 1992-1993, n° 1265.

Ainsi, placée dans l'ensemble de l'ordonnance, la mesure est conforme au but poursuivi et elle n'est pas proportionnée à celui-ci. Elle est d'ailleurs indispensable à un autre objectif, qui est l'objet de l'article 6 de l'ordonnance dès lors qu'il s'agit d'accorder une protection particulière à une catégorie de personnes qui excède des bénéficiaires du minimex et qu'il n'est donc pas possible, ainsi que le relève l'exposé des motifs, "d'obliger les communes à impliquer les C.P.A.S. dans cette question". La mission d'accompagnement que les communes doivent confier à l'organisme visé à l'article 6 suppose que celles-ci connaissent l'identité des personnes protégées. Il est exclu que cette divulgation puisse faire l'objet d'une quelconque publicité ; les personnes qui recevront l'information sont par ailleurs tenues au secret professionnel ».

32 Des arrêts récents de la Cour d'arbitrage développent à l'envi des considérations sur ces conditions en particulier sur la question de la proportionnalité [78]. On citera au premier chef, 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. Cet arrêt rappelle que 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* ». Sur cette base, l'arrêt analyse en particulier scrupuleusement pour chaque disposition incriminée le caractère nécessaire de celles-ci au regard des objectifs décrits [79]. Ainsi, la gravité des infractions recherchées justifiera des méthodes de recherche plus « invasives » et, à l'inverse, l'existence de méthodes alternatives moins attentatoires plaidera en faveur de l'utilisation de méthodes particulières de recherche. La nécessité de l'existence d'un juge indépendant et impartial compétent pour vérifier la légalité des procédures est soulignée. Dans l'affaire du décret de la Communauté flamande portant publication d'une liste noire de sportifs reconnus s'étant dopés, la Cour estime que « *la publication entreprise n'est pas nécessaire pour atteindre l'objectif poursuivi par le législateur décrétal, puisque cet objectif peut également être réalisable par des moyens moins dommageables pour les intéressés* » [80].

78. À noter également l'arrêt récent de la Cour de Justice des Communautés européennes du 20 mai 2003 (arrêt *Osterreichische Rundfunk e.a.* C 465/00 et C 139/01, points 57 et 81).

79. « *Il revient au législateur, sous le contrôle de la Cour, de formuler des dispositions qui autorisent le recours à ces méthodes de recherche de manière telle que l'atteinte aux droits fondamentaux qu'elles comportent soit limitée à ce qui est nécessaire pour atteindre l'objectif décrit* ». Comparer à propos du même raisonnement, l'attendu (B.5.5) de l'arrêt de la Cour d'arbitrage du 19 juillet 2005 : « *En prévoyant que l'aide matérielle indispensable au développement de l'enfant serait exclusivement octroyée dans un centre fédéral d'accueil, la disposition attaquée constitue une ingérence dans la vie privée et familiale de l'intéressé. Une telle ingérence doit donc répondre aux exigences de légalité et de prévisibilité posées par l'article 22 de la Constitution et par l'article 8 de la Constitution, poursuivre un but légitime et se trouver par rapport à ce but dans un juste rapport de proportionnalité* ».

On ajoutera que cette exigence d'un contrôle de proportionnalité sera d'autant plus critique que les données concernées sont des données sensibles, comme c'est le cas des données judiciaires que traite Phenix. Sans doute, les attendus de l'arrêt M.S. C/ Finlande rendu par la Cour européenne des droits de l'homme concernaient des données de santé, il est clair que le raisonnement y tenu vaut également pour d'autres données sensibles, comme les données judiciaires. Dans cette affaire, la Cour rappelle que la protection des données à caractère personnel et spécialement des données médicales revêt une importance fondamentale pour l'exercice du droit au respect de la vie privée et familiale garanti par l'article 8 de la Convention. « *Le respect du caractère confidentiel des informations sur la santé constitue un principe essentiel du système juridique de toutes les Parties contractantes à la Convention. Il est capital non seulement pour protéger la vie privée des malades mais également pour préserver leur confiance dans le corps médical et les services de santé en général* » [81].

33 **La non utilisation à des fins incompatibles** au regard de celles qui ont présidé à la collecte signifie qu'une finalité ne peut être détournée. Une fois annoncée, la finalité doit être respectée, c'est-à-dire que les données ne peuvent être utilisées de manière incompatible avec cette finalité.

L'article 4, § 1er de la loi précise cependant que la compatibilité doit tenir compte de tous les facteurs pertinents, « *notamment des prévisions rai-*

80. C.A., n° 16/2005, 19 janvier 2005, note d'observations R. Marchetti, *R.D.T.I.*, 2005, n° 22, pp. 129 et s.

81. Dans le même sens, C.E.D.H., 25 février 1997, *Rev. Dr. Santé*, 1997-1998, p. 314, note S. Callens, à propos de la décision d'un tribunal suivant laquelle les renseignements médicaux collectés dans le cadre d'un procès et concernant la séropositivité de la personne concernée tomberaient dans le domaine public 10 ans après la décision.

sonnables de l'intéressé et des dispositions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables ».

À titre d'exception à la règle de compatibilité des finalités, la loi précise en son article 4, § 1er que n'est pas réputé incompatible un traitement ultérieur à des fins historiques, statistiques ou scientifiques lorsqu'il est effectué conformément aux conditions fixées par le Roi [82].

34 Le **contenu du traitement** doit être proportionné à la finalité poursuivie. En d'autres termes, seules les données relevantes, c'est-à-dire adéquates, pertinentes et non excessives par rapport à la finalité déterminée poursuivie par le traitement peuvent être traitées. Ce principe recèle de nombreuses implications. Ainsi, on considérera comme excessive une donnée qui présente un risque d'atteinte disproportionnée par rapport aux intérêts individuels de la personne concernée. L'adéquation et la pertinence s'entendent du lien nécessaire et suffisant entre l'information traitée et l'objectif poursuivi par l'opération de traitement. Ainsi, s'il s'agit d'identifier la fonction d'une personne, nul n'est besoin d'avoir son adresse ou son état civil. Enfin, si un système d'information poursuit diverses finalités, on s'arrangera pour que les données traitées par le système soient stockées de telle manière que seules les données nécessaires à une finalité du système d'information et non à une autre soient accessibles aux personnes habilitées pour cette première finalité. Des règles de structuration du dossier et le contrôle des autorisations permettent ainsi que pour chaque finalité, les catégories d'utilisateur et des données rendues accessibles soient différemment définies.

35 La **qualité des données, leur exactitude mise à jour et leur effacement** ou anonymisation lorsqu'elles ne sont plus nécessaires à la finalité poursuivie s'entend d'une obligation de diligence [83]. Il est clair que l'exigence

82. Cf. à ce propos, les articles 2 à 24 de l'arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection des données à caractère personnel, *M.B.*, 13 mars 2001.

83. T. Leonard, *op.cit.*, note 84. Dans le même sens, parmi de nombreux auteurs, C. de Terwangne, *op. cit.*, p. 162 : « *La loi précise qu'il incombe au responsable du traitement de prendre toutes les mesures raisonnables pour que les données inexactes ou incomplètes, au regard des finalités poursuivies soient effacées ou rectifiées. C'est donc une obligation de moyens et non de résultat qui est mise à charge du responsable* ».

se comprendra différemment suivant le type d'opérations envisagées et les risques encourus par la personne concernée en cas d'utilisation de données inexactes, incomplètes ou non mise à jour.

2. *Les finalités de Phenix au regard des exigences de la loi dite vie privée*

a) Les finalités « communication interne » et « communication externe » (article 3)

36 L'article 3 distingue deux groupes de finalités : celles relatives aux communications internes et celles relatives aux communications externes. La nécessité de cette distinction voire, au sein de chaque groupe de finalités, de prise en considération de finalités plus déterminées encore, répond à la critique de la Commission de la protection de la vie privée relative à l'article 3 de l'avant-projet de loi qui regroupait « communication interne et externe » sous la même finalité.

> La Commission [84] écrivait :
>
> « À propos de la première finalité, "communication interne et externe requise par le fonctionnement de la justice", on note que cette mention est peu spécifique et couvre toutes les applications tant d'une administration que d'une entreprise. Le tableau annexé déjà cité, par lequel les auteurs du texte précisent chacune des finalités, n'envisage comme communications que les seules opérations ou actes de procédure qui marquent les diverses étapes de celle-ci. Ces communications correspondent certes à un traitement avec une finalité propre : "introduction et suivi d'un dossier" mais à cette première finalité, s'en ajoutent d'autres sous la rubrique large "communications internes et externes". La communication interne poursuit en effet d'autres finalités : recherche d'antécédents, d'éléments connexes au dossier. En outre, il est légitime de penser qu'au-delà des finalités liées aux dossiers judiciaires, le système d'information Phenix s'étendra à toutes les applications intranet : courrier électronique et "transferts de fichiers" que requiert le fonctionnement d'une organisation comme celle que constitue le pouvoir judiciaire ».

37 Le texte même de l'alinéa 1 semble d'ailleurs distinguer ces deux finalités de la communication interne : la première concerne la communication requise

84. Avis n° 11/2004, p. 81

pour le fonctionnement et la gestion des cours et tribunaux et de leur parquet. Ainsi, peut-on concevoir que les échanges de mails au sein de l'Intranet relatifs à la répartition des tâches ou à la vie du Palais au sens large, que la communication soit d'ordre professionnel ou privé relèvent de cette "communication interne". Sans doute, eût-il été plus avisé dès lors de prévoir un article supplémentaire pour ces échanges professionnels ou privés entre membres ou employés du pouvoir judiciaire. À l'égard de telles communications, il s'agirait de rappeler les principes dégagés par la Commission de protection de la vie privée à propos de la surveillance de l'utilisation des moyens électroniques de communication [85]. À défaut d'un tel article, c'est sans doute à cette première phrase qu'il faut rattacher cette communication interne.

38 La seconde partie de la phrase s'adresse aux traitements liés « *à la constitution ou à la gestion des dossiers de procédure* ». À propos de tels traitements, le délégué du ministre de la Justice évoque « la communication et le dépôt des pièces » visé par l'article 13 du projet de loi modifiant l'article 32*bis* du Code judiciaire. L'exemple surprend dans la mesure où il concerne une communication externe, en toute hypothèse, d'une transmission de données à caractère personnel venant d'une entité extérieure. On suppose dès lors que cette finalité vise plutôt la transmission au sein du pouvoir judiciaire (greffes, magistrats) des dossiers y introduits.

39 À propos du second type de finalités visées par l'article 3, à savoir les « communications externes », la lecture de l'alinéa 2 introduit également une distinction qu'il serait utile d'approfondir. Tant l'exposé des motifs [86] que les réponses du délégué [87] au rapporteur du Conseil d'État mentionnent exclusivement les communications nécessaires au déroulement des procédures judiciaires : la notification, la signification et la communication des actes

85. Avis d'initiative n° 10/2000 relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu du travail. Cet avis a donné lieu à l'arrêté royal du 12 juin 2002, rendant obligatoire la convention collective du 26 avril 2002 conclue au sein du Conseil national du travail relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau. Cet arrêté royal n'est pas applicable dans la fonction publique et *a fortiori* vis-à-vis du pouvoir judiciaire.

86. Exposé des motifs, p. 8.

87. Avis du Conseil d'État n° 37.943/2, p. 44.

requis par ces procédures [88]. Or, le texte laisse entrevoir le besoin de reconnaître d'autres traitements : ceux nécessaires à la « *collecte des données nécessaires pour l'élaboration et la gestion des dossiers judiciaires* ».

Ainsi, on peut songer à l'interrogation par le pouvoir judiciaire de bases de données administratives, comme le registre national, la banque carrefour des entreprises, le casier judiciaire [89], les registres de la direction de l'immatriculation des véhicules, le cadastre, les bases de données du fisc, etc. C'est à propos de ce second type de traitement, que la Commission de protection de la vie privée écrivait [90] « *Quant à la communication externe, elle n'est pas seulement celle entretenue avec les parties, elle peut se nourrir également de données collectées auprès d'administrations tierces ou d'autorités policières. Ce point est d'autant plus important que c'est précisément à propos de ces communications qui ont pour but d'aider les autorités judiciaires dans le travail d'investigation des faits que les risques d'atteinte à la vie privée et aux libertés des justiciables sont majeurs* ».

Cette considération de la Commission faisait écho à son souci exprimé d'emblée [91] : « *Au-delà des questions de protection des données sensu stricto, la Commission attire l'attention sur le fait que l'introduction des technologies dans les tribunaux, si elle facilite — et cela reste positif — le travail du juge et lui permet de rassembler facilement l'ensemble des informations relatives à un dossier*

88. Les deux textes cités aux notes précédentes mentionnent les différents actes de procédure pour lesquels communication externe est opérée : « *en ce qui concerne la communication externe, et plus précisément,*
- *la notification : art. 14 du projet de loi relatif à la procédure par voie électronique,*
- *la signification : art. 14 du projet de loi relatif à la procédure par voie électronique,*
- *le pli judiciaire : art. 19 du projet de loi relatif à la procédure par voie électronique,*
- *la signification en matière pénale : art. 51 du projet de loi relatif à la procédure par voie électronique,*
- *la requête : art. 5 et 26 du projet de loi relatif à la procédure par voie électronique,*
- *les conclusions : art. 33, 35 et 36 du projet de loi relatif à la procédure par voie électronique,*
- *les PV d'audience : art. 37 du projet de loi relatif à la procédure par voie électronique.*

89. Le Conseil d'État (Avis n° 37943/2, p. 44) demande que soit mentionnée expressément la loi du 8 août 1997 relative au casier judiciaire central qui régit la communication des décisions rendues en matière pénale et de défense sociale.

90. Avis n° 11/2004, p. 82.

91. Avis n° 11/2004, p. 80.

ou à un élément du dossier (ex : nombre de condamnations déjà encourues par la personne prévenue), accroît le pouvoir des parquets et tribunaux vis-à-vis des justiciables ; la volonté de maintenir un certain équilibre des intérêts entre le justiciable et l'appareil judiciaire plaide pour certaines limites dans le traitement des données et leur accès, en même temps que pour une transparence des circuits d'information existant dans l'appareil judiciaire en conformité avec les lois existantes ».

40 Sans doute, serait-il bon pour répondre à l'inquiétude ainsi exprimée, d'une part, que les flux d'information entre le pouvoir judiciaire et les banques de données de l'administration soient plus transparents [92] et que les conditions et modalités qui entourent cette possibilité d'interrogation soient progressivement précisées par le comité de gestion après avis du Comité de surveillance [93] et, d'autre part, que l'utilisation de telles interrogations soit portée à la connaissance du justiciable ou de son représentant.

b) Le répertoire des adresses judiciaires électroniques (article 4)

41 L'article 4 mentionne l'existence d'un traitement : « *La banque de données des adresses judiciaires électroniques* ».

Ce faisant, l'article 4 se réfère à l'article 16 du projet de loi relative à la procédure par voie électronique (art. 36, § 1er, 3° du Code judiciaire en projet) qui définit l'adresse judiciaire électronique comme étant : « *l'adresse de courrier électronique à laquelle une personne a accepté ou est réputée avoir accepté, selon les modalités fixées par le Roi, que lui soient adressés les dépôts, significations, notifications, avis et les communications* ».

L'idée est que les greffes, en collaboration avec le prestataire de services de communications agréé par le comité de gestion ou une autre instance

92. Tant la loi sur le registre national que sur la banque-carrefour des entreprises exige que le Comité sectoriel en charge du contrôle de ces institutions dresse un cadastre des flux entrants et sortants de ces bases de données, cadastre auquel le citoyen doit avoir accès.

93. On n'évoquera pas ici la question délicate des conflits de compétence qui pourraient exister dans ces cas entre comités sectoriels. Ainsi, l'autorisation d'accès au registre national est-elle une compétence du comité sectoriel « Registre national » ou du comité de gestion. Sans doute, sera-ce au président de la Commission de protection de la vie privée à trancher la question ?

désignée par le Roi [94] délivre une adresse judiciaire électronique à toute personne qui en fait la demande et qui par là même accepte de recevoir des documents judiciaires par voie électronique.

Le Roi peut, en outre, à terme, imposer que certaines catégories professionnelles « *qui à titre professionnel, à la requête de tiers ou d'une autorité judiciaire, posent des actes de procédure judiciaire soient tenues de poser et de recevoir des actes de procédure par voie électronique* » [95]. On vise ici les auxiliaires de justice.

Le répertoire des adresses judiciaires électroniques constituent un « annuaire » [96] de ces adresses.

Cet annuaire ne sera pas public mais accessible aux auxiliaires de justice, aux membres de l'Ordre judiciaire, ainsi qu'à d'autres personnes déterminées par le Roi. [97]

42 Cet annuaire doit être distingué des listes professionnelles. Afin néanmoins de permettre au greffe de vérifier si la personne qui fait une demande d'envoi de document à son adresse électronique [98] a bien la qualité d'avocat, de magistrat, de notaire ou de huissier qu'elle prétend avoir, ou qu'il n'est pas suspendu dans ses fonctions, le greffier aura la possibilité de consulter des listes professionnelles établies et tenues à jour de manière permanente,

- par la Cour de cassation, pour ce qui concerne les magistrats [99],
- par les Ordres des avocats pour ce qui concerne les avocats [100],

94. Cf. art. 10 du projet de loi dite « Procédure par voie électronique ».

95. *Id.*, art. 4, al. 2, 1°.

96. *Doc. parl.*, Ch., 2004-2005, 1645/001, p. 9.

97. Art. 4 loi Phenix.

98. Le projet de loi relatif à la procédure par voie électronique prévoit en effet en son article 4 la possibilité pour un auxiliaire de justice : huissiers, notaire, avocat de souscrire une adresse électronique et ainsi d'accepter que lui soient adressés les dépôts, significations, notifications et les communications. La finalité de la banque de données des adresses électroniques serait donc de permettre au pouvoir judiciaire d'entrer en contact aisément avec leurs auxiliaires pour la transmission des documents par voie électronique.

99. Art. 23 du projet de loi dite « Procédure par voie électronique ».

100. *Idem*, art. 24.

- par la chambre nationale des huissiers de Justice pour ce qui concerne les huissiers [101],
- par la chambre nationale des notaires pour ce qui concerne les notaires [102].

Contrairement au répertoire des adresses judiciaires électroniques, ces répertoires professionnels seront accessibles au public.

c) La gestion et la conservation des dossiers judiciaires (article 5)

43 Comme le note l'exposé des motifs [103], « *l'une des principales fonctions de Phenix est de permettre la gestion et la conservation des données judiciaires* ». L'alinéa 2 insiste sur le fait que les prescrits du Code judiciaire et du Code d'instruction criminelle et des dispositions particulières en ce qui concerne la composition de ces dossiers valables tant pour les dossiers papiers qu'électroniques permettent déjà de répondre aux questions : quelles sont les données traitées ? Quelle est la durée de conservation ? Qui peut y avoir accès tant en écriture qu'en simple consultation ? [104].

L'utilisation de l'outil informatique nécessite cependant quelques précisions supplémentaires confiées par l'alinéa 2 au Roi qui, dans les limites strictes des dispositions légales rappelées, détermine « *sur proposition du comité de gestion et après avis du comité de surveillance, les règles de pérennité des données, ainsi que les règles d'accès et d'authentification* [105] *d'accès aux dossiers judiciaires* ».

101. *Idem*, art. 25.

102. *Idem*, art. 53.

103. Exposé des motifs, p. 9.

104. Par exemple, on note sur ce point que le projet de loi relative à la procédure électronique décrit méticuleusement en ses articles 44 et s. à la fois la composition du dossier électronique en matière pénale, les règles d'accès et de gestion (qui peut retirer une pièce du dossier et selon quelle modalité) de création (qui décide de l'élaboration du dossier sous forme électronique ?) et de conservation. Les règles de consultation et de copie sont de même détaillées, ainsi que celles de transmission (art. 47 et s.).

105. On notera à cet égard, le rôle important que joueront les prestataires de service de communication, définis par l'art. 2, 4° du projet de loi relative à la procédure électronique comme suit : « *Le prestataire de services de communications : 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* » et dont la mission est fixée à l'article 10 de ce projet de loi :

d) Le rôle national (article 6)

44 Cette disposition prévoit l'attribution à chaque affaire portée devant l'Ordre judiciaire d'un numéro unique lors de son inscription au rôle national et confie au Roi, dans le respect des lois, le soin de fixer selon la même procédure que celle rappelée à l'article 5 les règles de pérennité des données, ainsi que les règles d'accès et d'authentification d'accès au rôle.

Le rôle national n'a pas de fonction proprement juridique : il constitue juste un instrument de gestion de l'outil informatique Phenix. Chaque dossier judiciaire reçoit un numéro unique pour tout le pays. Ce numéro est un numéro séquentiel, qui de lui-même ne donne aucune information sur le dossier aux personnes ne disposant pas d'un accès au dossier [106].

Il n'a dès lors pas vocation à être public.

45 Ce rôle doit être distingué du rôle tenu au greffe de chaque juridiction, régi par l'article 711 du Code judiciaire, lui-même en passe d'être modifié par l'article 27 du projet de loi procédure par voie électronique [107]. Celui-ci men-

« *§ 1er. Le prestataire de services de communication, doit répondre aux exigences suivantes :*
1° veiller à ce que les dates et heures d'envoi et de délivrance des actes de procédure puissent être déterminées avec précision ;
2° vérifier, par des moyens appropriés et légaux, l'identité des parties à la signification, à la notification ou à la communication ;
3° utiliser des systèmes et des produits fiables qui sont protégés contre les modifications et qui assurent la sécurité technique et cryptographique des fonctions qu'il assume ;
4° prendre des mesures pour garantir la confidentialité des données transmises tout au long du processus de communication des messages, ainsi que des données qu'il doit conserver ;
5° enregistrer toutes les informations pertinentes relatives aux communications effectuées pendant le délai utile de 30 ans, en particulier pour pouvoir fournir une preuve de la certification en justice ;
6° respecter les délais imposés par l'expéditeur afin de permettre à celui-ci de se conformer aux délais légaux ;
7° communiquer sans délai à l'expéditeur les données visées aux points 1° et 2°, ... ».

106. *Doc. parl.*, Ch., 2004-2005, 1645/001, p. 10. Le principe de proportionnalité du contenu (*supra*, n° 36) impose que seuls le lieu de dépôt du dossier et son numéro séquentiel soient repris dans le rôle national. Il ne paraît pas nécessaire d'y reprendre le nom des parties, ni la cause. Ce numéro d'identification unique peut apparaître comme une clé qui permet de suivre le dossier à la trace tout au long de son parcours judiciaire.

107. *Doc. parl.*, Ch., 2004-2005, 1701/001, p. 109.

tionne pour chaque cause inscrite, tout d'abord le numéro du rôle national qui lui est attribuée, ainsi que le nom des parties, le numéro de chambre où la cause est introduite, les dates des décisions intervenues, etc.

À propos du rôle des juridictions, on rappellera l'avis n° 22/2000 rendu le 28 juin 2000 par la Commission de la protection de la vie privée [108]. Cet avis concernait l'utilisation, par des sociétés de renseignement commercial, du rôle général des tribunaux du travail, dont l'article 719 du Code judiciaire prescrit la publicité. Il s'agissait en l'occurrence de prendre note du nom des employeurs en retard de paiement de leurs cotisations à l'O.N.S.S. et de transmettre ces noms à des organismes financiers.

L'avis rendu par la Commission porte sur des points fondamentaux. Il rappelle que la finalité du rôle créé par l'article 719 du Code judiciaire consiste à permettre aux tiers d'intervenir volontairement dans la procédure, non à des fins de renseignement commercial.

Il ajoute que le traitement de données publiques n'échappe pas à la garantie que constitue le principe de finalité : une donnée même rendue publique, concernant une personne physique, doit continuer à bénéficier d'une protection, celle-ci doit d'ailleurs être renforcée vu les performances techniques de l'outil informatique et que le traitement mis en œuvre par les sociétés ne semble pas conforme à l'article 4, § 1er, 2° de la loi relative à la protection de la vie privée qui prévoit que les données doivent être exactes et si nécessaire, mises à jour. Or la collecte des données au seul moment de l'assignation en justice est dangereuse car aléatoire.

Enfin, il désigne le responsable du traitement et rappelle ses obligations. Les articles 4, § 2 et 16, § 4 de la loi du 8 décembre 1992 précisent les devoirs des procureurs généraux [109] : ils doivent veiller à ce que les données du rôle ne soient pas utilisées de manière incompatible avec la finalité du traitement, et ils doivent prendre les mesures techniques et d'organisation pour protéger les données à caractère personnel et en déduit son obligation d'assurer la sécurité du traitement.

108. Cet avis est commenté notamment par J. Hubin, « Les relations Barreau-Palais », in *Cabinets d'avocats et technologies de l'information, op. cit.*, pp. 369 et s.
109. En effet, la tenue du rôle relève de leur responsabilité.

e) Les banques de données jurisprudentielles (articles 7 et s.)

46 L'article 7 distingue la banque de données jurisprudentielles « interne », dont la finalité est une consultation limitée aux membres du pouvoir judiciaire des décisions rendues et celle « externe » caractérisée par la libre accessibilité à tous des décisions « *ayant une importance pour la connaissance et l'évolution du droit* ».

Le propos de Madame de Terwangne, consigné dans ce même ouvrage, sur ce second type de banques de données jurisprudentielles justifie que soit analysée la seule banque de données de jurisprudence interne, ou plutôt les seules banques de données internes dans la mesure où l'article 7 rattache à chaque juridiction celles-ci.

47 La finalité énoncée est en effet de permettre aux différents membres d'une juridiction de traiter leurs dossiers judiciaires. À l'inverse de la banque externe qui ne se veut pas exhaustive et ne reproduit que des jugements rendus anonymes, la banque interne reproduit l'intégralité des jugements et n'est accessible qu'aux seuls membres de la juridiction qui les a émis et ce à la seule fin, dit l'article 8, alinéa 2, « *d'exercer leur tâche professionnelle* », encore faut-il s'entendre sur le sens de ces termes.

L'historique du texte et la discussion en commission du Sénat permettent de mieux comprendre l'exacte signification de la finalité ainsi décrite. L'avant-projet de loi ne mentionnait pas les restrictions d'accès à la banque jurisprudentielle interne. Il était alors précisé que l'accès à une telle banque de données s'opérait selon des modalités fixées par le comité de gestion et le comité de surveillance qui « *prennent en compte les règles relatives à la protection des données* ». La Commission de protection de la vie privée s'était émue du caractère vague de cette disposition qui permettait à un juge de pouvoir rassembler facilement l'ensemble des informations judiciaires relatives à une personne citée devant lui. Ainsi, telle personne, demandeur, devant une juridiction du travail pour licenciement abusif, a pu avoir été déjà condamné par la juridiction pénale d'un autre ressort pour ivresse au volant, par le juge de paix pour troubles de voisinage, etc. La Commission s'inquiétait de cette consultation interne qui accroissait le pouvoir des parquets et des tribunaux vis-à-vis des justiciables [110].

110. Avis n° 11/2004, p. 80.

La restriction par le projet de loi de la consultation interne à la seule juridiction répondait à cette inquiétude. En Commission du Sénat [111], deux positions se sont exprimées à ce propos. Le sénateur H. Vandenberghe a estimé devoir préciser que le mot « juridiction » ne s'étendait pas pour une cour d'appel à l'ensemble des juridictions du ressort de la cour d'appel alors que Mme t'Serclaes soulignait au contraire l'intérêt pour la justice d'un accès à l'ensemble des décisions relatives à un justiciable, ce qui permet une « vision globale du problème ». Il s'agissait en d'autres termes de permettre à un magistrat de mieux cerner le profil de son justiciable en s'aidant des données de son passé judiciaire [112].

À ces interventions, le ministre et son délégué répondent que telle n'est pas la finalité de cette banque jurisprudentielle interne [113] qui doit simplement permettre aux membres d'une juridiction entendue au sens strict d'assurer une certaine unité de leur jurisprudence. Ainsi, cela permet 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. Si telle est la finalité précise de la banque jurisprudentielle interne [114], on peut s'interroger sur la nécessité d'y faire figurer les données des justiciables de manière nominative, ce que la sénatrice C. Nyssens proposait d'ailleurs.

f) Les statistiques internes et externes (articles 10 et s

48 Suite à l'avis de la Commission de protection de la vie privée [115], sur l'avant-projet de loi, le texte relatif aux traitements statistiques a été profondément

111. Lors de la réunion du 17 mai 2005 de la Commission Justice au Sénat (Doc. Sénat n° 3-1163/3).

112. Extrait des débats en commission « Justice » du Sénat « M. Hugo Vandenberghe estime que le texte manque de clarté en ce qui concerne les personnes ayant accès à la base de données interne, que visent les mots "la juridiction". La ministre répond que l'accès n'est autorisé qu'aux membres de la juridiction elle-même (le tribunal de première instance, par exemple). M. Hugo Vandenberghe s'étonne que la cour d'appel n'ait pas accès aux décisions des tribunaux de son ressort ».

113. ... c'est le rôle, dit le ministre, du « casier judiciaire central ».

114. Extrait des débats en Commission de la Justice du Sénat : « *Cette distinction, affirme la Ministre, s'opère en fonction de la finalité poursuivie. La première banque de données a pour but de permettre aux magistrats d'une même juridiction d'assurer une certaine unité de jurisprudence. Dans ce cas, l'accès est autorisé à l'ensemble des décisions rendues par la juridiction, mais est limité aux seuls membres de la juridiction* ».

115. Avis n° 11/2004, p. 87.

remanié. Il s'agissait bien évidemment ici de protéger les membres du pouvoir judiciaire contre les utilisations statistiques qui auraient pu mettre en cause la recevabilité de certains ou révéler les interprétations originales ou tendances suivies par l'un ou l'autre.

Une distinction est donc proposée à l'article 10 entre statistiques à usage interne et celles à usage externe. Ces dernières doivent, selon le prescrit de l'article 12, alinéa 2, être préalablement « anonymisées » ou codées selon des modalités particulières déterminées par le Roi sur proposition du comité de gestion, après avis du comité de surveillance.

Quant aux premières, on distingue des statistiques élaborées à la demande du chef de corps (le président d'un tribunal ou d'une cour d'appel, le procureur général) qui doivent porter sur la bonne gestion d'une juridiction ou d'un parquet : ainsi, les rentrées financières, le nombre d'heures de travail prestées par le greffe, etc. et celles demandées par le ministre, un ou plusieurs chefs de corps, le Conseil supérieur de la Justice ou le comité de gestion qui « établissent de manière globale la charge de travail de l'Ordre judiciaire, le fonctionnement des institutions judiciaires et sur les affaires portées devant les autorités judiciaires ». Les précisions ainsi apportées permettent d'éviter le flou antérieur de l'avant-projet qui ajoutait le droit d'élaborer des statistiques « sur la charge de travail et sur tout autre sujet » [116].

g) L'aide à la gestion et l'administration des institutions judiciaires (article 14)

49 L'alinéa 1 de la loi définit ce qu'il faut entendre par cette dernière finalité. Il s'agit de la gestion des ressources humaines (par exemple, heure de présence des membres du pouvoir judiciaire, horaire de vacances, liste et barèmes des

116. Ce flou avait été violemment critiqué par la Commission de la protection de la vie privée (p. 87) en les termes suivants : « *La Commission s'interroge sur le flou de la disposition : Qu'entend-on par critères d'élaboration des statistiques ? La notion de statistiques "globales" vise sans doute des statistiques portant sur l'ensemble de l'activité des tribunaux, ce qui n'exclut pas des statistiques aboutissant à des données non anonymes ou utilisant de telles données. L'objet même des enquêtes est peu défini : qu'entend-on par "sur tout autre sujet" ? Sans doute, ceci serait à préciser. Il ne peut s'agir en tout cas que de statistiques permettant d'apprécier le fonctionnement du pouvoir judiciaire et répondant à un besoin d'information du public ou de définition de politique à mener au sein du secteur judiciaire (lutte contre l'encombrement du pouvoir judiciaire, définition de nouvelles compétences, etc.). Les projets d'enquête devraient donc être soumis au comité de surveillance* ».

personnes employées ou nommées, etc.), la gestion de la documentation (les ressources de la bibliothèque du palais, la liste des emprunteurs, etc.), la gestion des fournitures et la comptabilité (rentrées financières et sorties).

Ces précisions avaient été demandées par la Commission de la protection de la vie privée qui s'inquiétait à juste titre du texte initial de l'avant-projet, jugé trop flou.

B. Les autres dispositions de la loi vie privée et leur application aux traitements mis en place par Phenix

50 Sans vouloir être exhaustif, notre propos souligne deux types de prescrits de la loi dite vie privée, dont l'application aux traitements mis en place par Phenix n'est pas évidente. Les premiers concernent les **droits subjectifs accordés à la personne concernée**, qu'il s'agisse du justiciable le plus souvent mais également des auxiliaires de justice voire des membres de l'Ordre judiciaire. Ils sont nombreux et vont du simple droit à l'information au droit à l'opposition. Le second type de prescrits concerne certaines obligations mises à charge du responsable, ainsi l'obligation de sécurité ou de notification.

1. *Les droits subjectifs de la personne concernée*

51 La législation de protection des données accorde à la personne concernée un certain nombre de droits subjectifs destinés à assurer la transparence des traitements et à lui permettre un contrôle de ceux-ci.

L'obligation d'information de la personne concernée prévue à l'article 9 permettra, dans un deuxième temps, à la personne ainsi informée d'**accéder** au contenu du traitement voire à sa logique suivant l'article 10. Si l'accès révèle quelque erreur ou tout autre manque de qualité de la donnée, la personne pourra exiger la **rectification** de la donnée conformément aux articles 12 et s., en particulier il disposera d'une action comme en référé devant le président du tribunal de 1re instance. Enfin, la personne concernée dispose du droit d'opposition dans certains cas précis selon l'article 12, § 1, alinéa 2.

52 L'octroi de tels droits cède, on le conçoit, vis-à-vis de certains traitements. L'article 3 prévoit ainsi des exceptions, d'une part (§ 4), en fonction de la

qualité de certains responsables de traitements : sûreté de l'État, le service général de renseignement, l'autorité de sécurité et le comité permanent de contrôle des services de renseignements, d'autre part (§ 5), en fonction de la finalité des traitements, ceux gérés par les autorités publiques dans le cadre de leurs missions de police judiciaire ou de police administrative.

Le pouvoir judiciaire est-il, au terme de cet article, exonéré de l'ensemble de ces devoirs d'information ? Aucune dérogation ne le vise explicitement. Sans doute, peut-on considérer que certains traitements liés à certaines juridictions en particulier pénales poursuivent les missions visées au paragraphe 5 [117] mais, au-delà, la question ne doit-elle pas être posée ? Suffit-il d'affirmer que les procédures suivies par les juridictions, et ce en vertu des Codes judiciaire et d'instruction criminelle, prévoient de manière originale leurs propres obligations d'information et de transparence pour décréter que ces dispositions de la loi du 8 décembre 1992 ne sont pas applicables aux traitements entourant ces procédures ? Sans aucun doute, lorsque le Code judiciaire ou le Code d'instruction criminelle prévoient expressément des modalités particulières tendant à l'information de la personne concernée, en l'occurrence le justiciable, ou offrant à cette dernière un droit d'accès.

Sans être exhaustif, on cite l'article 61 du Code d'instruction criminelle qui prévoit (61*bis*) l'information du justiciable : « *le juge d'instruction procède à l'inculpation de toute personne à l'égard de laquelle il existe des indices sérieux de culpabilité. Cette culpabilité est faite lors d'un interrogatoire ou par notification à l'intéressé* ». En ce qui concerne le droit d'accès (61*ter*), on cite :

> « § 1er L'inculpé non détenu et la partie civile peuvent demander au juge d'instruction de consulter le dossier (...)
>
> § 2 Le juge d'instruction peut interdire la communication de certaines pièces si les nécessités de l'instruction le requièrent...
>
> § 3 (...) le dossier est mis à disposition en original ou en copie pour être consulté (...) le greffier donne avis au requérant du moment où le dossier pourra être consulté (...) ».

Quant au droit de correction, l'art 61*quinquies* énonce : « *l'inculpé et la partie civile peuvent demander au juge d'instruction l'accomplissement d'un acte d'instruction complémentaire...* ».

117. Ceci est loin d'être évident dans la mesure où la procédure judiciaire au fond peut difficilement être qualifiée de mission de police.

En matière de procédure civile, on se réfère par exemple à l'article 736 du Code judiciaire qui prévoit que *« les parties se communiqueront les pièces avant leur emploi (...) »* ou à l'article 745 qui dispose que *« toutes conclusions sont adressées à la partie adverse (...) »*. Le droit d'avoir copie du jugement le concernant n'est-il pas en ce sens une préfiguration du droit d'accès ?

53 Mais au-delà, vis-à-vis des autres personnes concernées ou d'autres traitements pour lesquels le Code judiciaire ou le Code d'instruction criminelle ne prévoient pas de solution spécifique, l'argument suivant lequel en matière judiciaire les droits subjectifs des personnes concernées ne s'exercent pas vu la nature même du pouvoir judiciaire convainc peu au moment où la loi « Phenix » proclame la soumission des traitements qu'elle crée, à la loi de protection des données à caractère personnel. L'exception ne vaut que vis-à-vis des données relatives à de telles procédures, or le système Phenix envisage d'autres traitements que ceux-là, ainsi, lorsqu'il crée des banques de données jurisprudentielles, des statistiques ou se réfère à des bases de données listant les membres des juridictions ou les différents auxiliaires de justice.

Il nous revient donc de procéder à l'analyse des différents droits subjectifs octroyés par la loi de 1992.

54 Le premier oblige le responsable du traitement à **informer**, suivant le prescrit de l'article 9, la personne concernée de l'existence du traitement soit au moment de la collecte si celle-ci a lieu auprès de la personne concernée, soit au plus tard lors de la communication des données.

L'information porte sur une série de rubriques et rien n'est prévu quant aux modalités par lesquelles s'accomplit le devoir d'information.

Sans doute, certaines exceptions à ce devoir d'information existent. Peut-on les envisager dans le cadre des traitements relatifs à Phenix ?

La collecte directe prévoit une seule exception : le cas où la personne est déjà informée. On notera que, suivant le type de personne concernée, les hypothèses de collecte directe vaincront. Elles sont rares, réduites à la disposition directe ou au témoignage à quelque stade de l'instruction ou du procès, dans le cas de données relatives à un justiciable. Elles sont plus fréquentes à propos des auxiliaires de justice puisque toute demande d'accès à un dossier, toute introduction d'une instance, toute transmission de pièces

ou de conclusions donne lieu à une collecte de données. Sans doute, peut-on imaginer que les auxiliaires de justice soient dûment informés avant même la collecte des finalités des données qui leur seront réclamées par la justice ou plus spécifiquement par le système d'informations Phenix. On peut imaginer de même que la formation de magistrats amène ces derniers à prendre connaissance de la collecte qui est faite de données les concernant et des finalités d'utilisation de ces données.

En cas d'obtention de données, via des tiers, le devoir d'information cède suivant l'article 9, § 2, point b, lorsque *« l'enregistrement ou la communication des données à caractère personnel est effectué en vue de l'application d'une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance »*. Cette exception est cependant soumise, selon le texte de la loi, à des conditions à déterminer par arrêté royal. La lecture des articles 28 et suivants de l'arrêté royal vise à ce propos différentes hypothèses mais aucune ne semble être relevante vis-à-vis du pouvoir judiciaire.

55 Le deuxième droit subjectif octroie à la personne concernée le **droit d'accéder** [118] à une série d'informations relatives au traitement entrepris à son propos. Ainsi, la personne justifiant de son identité recevra communication à la fois du fait que des données sont traitées à son égard, des finalités du traitement, des catégories de destinataires mais également et sous forme intelligible des données faisant l'objet des traitements ainsi que l'information disponible sur l'origine du traitement. Si la décision à prendre par l'autorité devait être automatisée, la personne concernée doit connaître la logique suivie par un tel traitement automatisé.

Un tel droit d'accès peut-il exister vis-à-vis des données détenues par le pouvoir judiciaire ? Hormis les cas où les dispositions du Code judiciaire ou du Code d'instruction criminelle dispensent le responsable du suivi des prescriptions de la loi de 1992 ou plutôt offrent un substitut à ces pres-

118. À noter, et ceci est important dans le cas qui nous occupe, que ce droit d'accès doit s'exercer sans contrainte. Il serait en effet dangereux et abusif pour un employeur d'exiger que le candidat employé fasse exercice de son droit d'accès pour prouver l'inexistence de tout jugement à son propos ou simplement le fait d'être fiché à un endroit quelconque de l'appareil judiciaire. La même remarque vaut à propos du casier judiciaire dont l'extrait est trop facilement demandé par des employeurs ou autres prestataires de services sans que cette exigence ne réponde à un intérêt légitime de la part du demandeur ou en tout cas d'un intérêt prépondérant sur celui de la personne concernée.

crits [119], le droit d'accès défini à l'alinéa précédent sera d'application. On regrettera que les exceptions prévues par l'article 13 de la directive européenne de 1995 n'aient pu trouver application [120]. Certaines auraient pu être invoquées, en particulier l'exception relative à la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie [121], celle relative à la protection de la personne concernée ou des droits et libertés d'autrui chaque fois que le droit d'accès permettraient la prise de connaissance de faits concernant autrui et nuiraient à ce dernier.

56 On évoquera pour mémoire les droits de correction et d'opposition dont l'application permettrait à un justiciable, à un auxiliaire de justice et à un membre du pouvoir judiciaire lorsqu'ils sont concernés par le traitement d'exiger du pouvoir judiciaire la suppression, la rectification ou le complément de données à caractère personnel.

Enfin, la loi de 1992 confère à la personne concernée en litige avec le responsable du traitement le droit de saisir le président du tribunal de première instance siégeant comme en référé [122] de « *toute demande relative au droit accordé par ou en vertu de la loi, d'obtenir communication de données à caractère personnel, et de toute demande tendant à faire rectifier, supprimer ou interdire d'utiliser toute donnée à caractère personnel inexacte ou, compte tenu du but du traitement, incomplète ou non pertinente, dont l'enregistrement, la communication ou la conservation sont interdits, au traitement de laquelle la personne s'est opposée ou encore qui a été conservée au-delà de la période autorisée* ». L'attribution de compétences à la Cour de cassation par la loi annexe à la loi Phenix en matière d'annulation des actes du Comité de gestion « *qui excéderaient ses pouvoirs, seraient contraires aux lois* (en l'occurrence à la loi vie privée) ou pris de manière irrégulière ne remet pas en cause de telles compétences présidentielles conférées par la loi de 1992, selon les débats parlementaires [123]. Le souci des auteurs de la loi de donner à la loi de 1992 sa pleine efficience pourrait cependant entraîner quelques difficultés dans la pratique, lorsque le président du tribunal de première instance saisi conformément à l'article 14 de la loi serait amené à contrôler les actes de juridictions hiérarchiquement supérieures ou aurait à statuer sur la demande d'accès ou de rectification émanant d'un magistrat.

119. À cet égard le passage de l'exposé des motifs (p. 23) qui note : « *En effet, ..., le droit d'accès au dossier judiciaire est régi par les dispositions du Code judiciaire ou du Code d'instruction criminelle. Pour les traitements de données qui ne sont pas régis par les Codes judiciaire ou d'instruction criminelle, comme le répertoire des adresses judiciaires électroniques, la loi délègue au Roi le pouvoir de décider, sur proposition du comité de gestion et après avis du Comité de surveillance, des modalités d'accès* ».

120. Ces exceptions valent également pour le droit à l'information sur l'existence du traitement et au droit de rectification.

121. ...par exemple, d'auxiliaires de Justice ayant cherché à abuser de leur accès à tels ou tels traitements mis en place par Phenix.

122. Sur la signification de cette procédure, lire T. Leonard, obs. sous Civ. Bruxelles (prés.), 22 mars 1994, *J.T.* 1994, p. 843.

2. *Les obligations du responsable du traitement*

a) Un préliminaire : Qui est le responsable du traitement ?

57 Aux termes de l'article 1er, § 4, alinéa 1er de la loi du 8 décembre 1992 relative à la protection des données à caractère personnel, le responsable de traitement est « *la personne physique ou morale, l'association de fait ou l'administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel* ». L'alinéa 2 du même article ajoute que « *lorsque les finalités et les moyens du traitement sont déterminés par ou en vertu d'une loi, d'un décret ou d'une ordonnance, le responsable du traitement est la personne physique, la personne morale, l'association de fait ou l'administration publique désignée comme responsable du traitement par ou en vertu de cette loi, de ce décret ou de cette ordonnance* ».

La loi Phenix ne désigne toutefois pas expressément de responsable de traitement et on peut le regretter [124]. Contrairement à d'autres lois [125], elle n'institue en outre aucun organe doté de la personnalité civile.

123. *Supra*, n° 12, la référence citée lors de l'analyse des organes de Phenix et de leurs compétences.

124. Cf. la jurisprudence de la Commission de la vie privée à cet égard : « *La détermination explicite du responsable de traitement dans la loi résulte également indirectement de la jurisprudence de la Cour européenne des droits de l'homme selon laquelle des ingérences au droit à la vie privée prévues par une loi en vertu de l'article 8, § 2 de la C.E.D.H. doivent l'être en vertu d'une loi accessible et prévisible (...) au vu de ce qui précède et du fait que le responsable de traitement constitue une pierre angulaire de la L.V.P., la Commission considère que la détermination explicite du nom du responsable de traitement doit être reprise dans le dispositif du projet d'A.R. afin que cette disposition légale réponde au caractère de prévisibilité exigé par la loi et confirmé par la jurisprudence de la Cour* » (Commission de protection de la vie privée, avis 15/2005, 19 octobre 2005, p. 11).

Dans son avis sur les projets de loi Phenix, la Commission de protection de la vie privée considère que « *Le S.P.F. Justice doit agir comme un sous-traitant de l'Ordre judiciaire au sens du paragraphe 5 de l'article 1er de la loi de 1992, soumis aux dispositions de l'article 16, § 1 de la loi de 1992. En d'autres termes, le S.P.F. Justice est à considérer comme l'administration agissant pour le compte du pouvoir judiciaire, véritable responsable des traitements du système Phenix, et dans le cadre strict des missions qui lui sont confiées* ». La Commission ajoute qu'en application de l'article 16, § 1 de la loi de 1992, un contrat entre l'Ordre judiciaire et le S.P.F. Justice devrait préciser les missions confiées à ce dernier et en fixer ses responsabilités » [126].

58 Nous ne partageons pas entièrement l'avis de la Commission sur ce point. En effet, dans les multiples opérations de traitement qui seront opérées au moyen du système d'information Phenix, il faut distinguer deux types de traitements distincts : le traitement structurel constitué par le système d'information Phenix et les traitements fonctionnels opérés à l'aide du système Phenix tels que la gestion des dossiers judiciaires, dont le contenu et la gestion appartiennent exclusivement au magistrat en charge du dossier. La loi donne dès lors au comité de gestion le pouvoir de déterminer les moyens du traitement Phenix lorsque ceux-ci sont structurels (s'inscrivant dans une certaine permanence) tandis que les moyens fonctionnels (telle une prise de décision d'utiliser la structure à telles fins...) sont du ressort des magistrats même en charge d'un dossier.

C'est ainsi que dans le traitement de gestion des dossiers judiciaires institué par l'article 5 de la loi Phenix du 10 août 2005, chaque magistrat, dans l'exercice de ses compétences juridictionnelles, est responsable du traitement que constitue son dossier judiciaire. Il veille au respect des principes de la loi vie privée dans les traitements qu'il fait des données judiciaires. L'obligation de respecter la loi vie privée ne constitue en aucun cas une immixtion dans la fonction juridictionnelle du pouvoir judiciaire car les obligations qu'elle impose ne touchent pas à cette fonction juridictionnelle pour laquelle il bénéficie de l'indépendance constitutionnelle. L'article 151 de la Constitution proclame en effet l'indépendance des magistrats en ces termes : « *Les juges sont indépendants dans l'exercice de leurs compétences juridictionnelles. Le ministère public est indépendant dans l'exercice des recherches et poursuites individuelles, sans préjudice du droit du ministre compétent d'ordonner des poursuites et d'arrêter des directives contraignantes de politique criminelle* ».

125. L'article 1er de la loi du 15 janvier 1990 relative à l'institution d'une banque-carrefour de la sécurité sociale dispose : « *Sous la dénomination banque-carrefour de la sécurité sociale, il est créé auprès du S.P.F. Sécurité sociale un organisme public doté de la personnalité civile dénommé ci-après banque carrefour* ».

126. *Doc. parl.*, Ch., 2004-2005, 1646/001, pp. 94-95.

En ce qui concerne les moyens structurels mis à disposition pour la gestion et la conservation des dossiers judiciaires, l'article 5 prévoit qu'il appartient au comité de gestion de proposer les règles de pérennité de données, d'accès et d'authentification d'accès aux dossiers judiciaires. Ceci est en effet nécessité par l'informatisation de la procédure où l'accessibilité et la disponibilité des données sont plus importantes qu'avec le support papier. Le comité de gestion devra donc veiller à assurer le respect des obligations de sécurité et de confidentialité de type technique que lui impose l'article 16 de la loi vie privée (limiter l'accès du personnel aux seules données nécessaires, prise de mesures techniques requises pour protéger les données particulières que constituent les données « judiciaires ») [127]. Quant aux mesures de sécurité et de confidentialité de type organisationnelle également imposées par l'article 16 de la loi vie privée (telle l'interdiction de prêter sa carte d'accès [128] au système d'information, de ne pas divulguer ses mots de passe...), le comité de gestion devra éveiller l'attention des magistrats sur la nécessité de les appliquer.

60 Le Rôle national visé à l'article 6 doit être considéré comme une mesure structurelle relevant de la compétence du comité de gestion. Il n'a en effet pas de fonction juridique et constitue uniquement un instrument de gestion de Phenix. De plus, il ne contient que les numéros uniques attribués à chaque dossier judiciaire lors de l'introduction d'une affaire devant une juridiction [129]. C'est le motif pour lequel, en vertu de l'article 6 de la loi Phenix, il appartient au comité de gestion de proposer les règles de pérennité de données, d'accès et d'authentification d'accès au rôle national.

127. Cela est d'ailleurs concrétisé par l'article 19 de la loi Phenix.

128. En l'occurrence, sa carte d'identité électronique.

129. Art. 711 du Code judiciaire modifié par l'article 27 du projet de loi relatif à la procédure par voie électronique, *Doc. parl.*, Ch., 2004-2005, 1701/001, p. 109.

Concernant les traitements statistiques, les chefs de corps seront responsables du traitement de données à des fins de statistique interne ainsi qu'il ressort de l'article 11 de la loi Phenix. Exceptionnellement le comité de gestion se voit attribuer une mesure fonctionnelle qu'est la publication ou la communication de statistique externe.

Enfin, en cas de plainte, c'est l'État belge représenté par la ministre de la Justice qui assumera en justice les conséquences de la responsabilité des organes mis en place par Phenix.

Comme on le voit, l'application de la loi vie privée et la détermination des différents responsables de traitements au système d'information Phenix et au traitement informatisé des dossiers judiciaires traités respecte le principe fondamental de la séparation des pouvoirs.

b) Les obligations du responsable du traitement : la sécurité et la déclaration des traitements

61 L'obligation mise à charge du responsable d'assurer la sécurité des données au sens le plus large, c'est-à-dire de garantir non seulement la confidentialité des données mais leur fiabilité et leur intégrité, est sans doute la première obligation à rappeler. Dans la mesure où le responsable, selon notre analyse [130], est le Comité de gestion, en ce qui concerne du moins les traitements correspondants aux moyens structurels, c'est à lui que revient la tâche de prendre ces mesures. L'article 17, alinéa 9 lui confie d'ailleurs le soin de proposer au Roi, après avis du Comité de surveillance, les règles d'accès et d'authentification d'accès aux dossiers électroniques de procédure et aux données contenues dans ce système. C'est lui qui, selon l'alinéa 10 du même article, « *certifie la conformité des documents qui ont été convertis ou placés sur un support électronique* ». Enfin, l'article 19 de la loi confie des missions de contrôle qui correspondent précisément au contenu de l'obligation de sécurité : « *contrôle de l'entrée de locaux où se trouvent les installations pour les traitements de données, contrôle de mémoire des ordinateurs traitant des données, contrôle des supports sur lesquels ces données sont stockées, contrôle de l'introduction des données, ...* ».

130. Voir *supra*, n[os] 60 et s.

De telles obligations sont de diligence et sanctionnées pénalement [131]. Pour mesurer la portée de ce devoir, le juge — en l'occurrence, serait-ce la Cour de cassation [132] ? — évaluera les efforts entrepris au regard des règles de l'art en tenant compte de la nature des données, des risques inhérents au système d'information choisi et de coûts raisonnables [133]. La nature particulièrement sensible de certaines données propres à certains traitements, la nature du réseau couvrant l'ensemble du secteur judiciaire et surtout le risque potentiel de dommages graves en cas d'insuffisance ou de violation des mesures de sécurité plaident pour des mesures de sécurité tant organisationnelles que techniques sévères.

62 L'obligation de sécurité telle que décrite à l'article 16 de la loi de 1992 se décline en divers contenus. Premièrement, le responsable, en l'occurrence le comité de gestion, veillera à ce que les personnes agissant sous son autorité n'aient la possibilité d'accéder à et d'utiliser que les seules données dont elles ont besoin pour exercer leurs fonctions. Cela impliquera la gestion de la délivrance de clés d'accès particulièrement robustes et on songe tout naturellement à la signature électronique utilisée comme moyen d'authentification même si la généralisation de l'utilisation de la carte laisse craindre que son porteur ne se laisse aller à divulguer la clé secrète ou le code PIN capable de déclencher le code secret. La gestion des codes d'accès (key management) est une autre dimension du problème. Il est clair également qu'au regard de chaque autorisation doit correspondre une définition des données auxquelles la personne peut accéder et l'implantation de mesures techniques visant à prévenir tout dépassement par une personne autorisée des limites de son autorisation.

La mise au courant des personnes agissant sous son autorité des prescrits légaux en matière de protection des données doit être opérée par le res-

131. Article 38 de la loi du 8 décembre 1992.

132. Rien n'est moins sûr dans la mesure où la Cour a, selon l'alinéa nouveau introduit par la loi Phenix 2 dans l'article 610 du code judiciaire, une simple compétence d'annulation des actes du comité de gestion qui excéderaient ses pouvoirs, seraient contraires aux lois ou pris de manière irrégulière. Or dans ce cas, il s'agirait d'une action en responsabilité civile voire pénale dirigée contre le responsable d'un traitement et en définitive l'État pour non respect de l'obligation de sécurité.

133. L'article 16, § 4 se réfère « *à un niveau de protection adéquat compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.* ».

ponsable du traitement. De même faudra-t-il veiller à ce que les personnes qui ont accès aux données sensibles, en l'occurrence les données judiciaires, soient tenues d'une obligation légale ou contractuelle de confidentialité [134].

On ajoute la prise de mesures d'ordre divers pour se prémunir contre la perte accidentelle de données, contre la destruction, la modification, l'accès ou tout autre traitement de données accidentel ou non autorisé. Qu'il s'agisse de mesures organisationnelles visant tant à prévenir (ne pas transmettre votre code d'accès et veiller à le modifier de temps en temps, comme le permet le logiciel de gestion fourni avec la carte d'identité électronique, éteindre l'ordinateur en sortant des lieux du travail, ...) qu'à sanctionner tout non respect des règles (sanction contractuelle, voire pénale) ou qu'il s'agisse de mesures techniques (anti-virus de qualité à jour, firewall, utilisation de logiciels de détection d'erreurs, conservation des traces d'identification lors de l'accès, ...).

63 Enfin, on rappelle le prescrit de l'article 16, § 1er en cas de choix de sous-traitant, c'est-à-dire d'une personne non placée sous l'autorité du responsable et à laquelle des missions de traitement des données sont confiées. Ainsi, une société de maintenance ou une entreprise privée offrant un service de back up pour des traitements opérés au sein de Phenix constituent des sous-traitants. À cet égard, on s'interroge : les ordinateurs du S.P.F. Justice qui stockent la plupart ces données centralisées par Phenix et constituent les serveurs pour les applications locales des magistrats ou des greffes, ne sont-ils pas placés sous l'autorité d'un tiers, le S.P.F. Justice agissant pour compte du comité de gestion et au delà du pouvoir de gestion ? L'article 16, § 1er exige que le sous-traitant ne soit pas choisi à la légère, offre des garanties suffisantes au regard des mesures de sécurité technique et organisationnelles qu'exige le traitement et enfin signe un contrat par lequel il s'engage à ne pas traiter les données pour son propre compte et qui fixe la responsabilité du sous-traitant vis-à-vis du responsable du traitement.

Toutes ces mesures de sécurité pourraient amener le Comité de gestion à désigner un préposé à la protection des données, agent indépendant chargé de veiller au respect des obligations imposées par la loi de 1992 dont le statut réclamé par l'article 17 de cette loi n'a toujours pas été défini. On

134. Article 25, 3° de l'arrêté royal du 13 février 2001

note que dans d'autres législations à propos du gouvernement électronique, le législateur n'a pas hésité à obliger les institutions à se doter d'un conseiller en sécurité ou d'un conseiller en sécurité et à la protection de la vie privée [135].

64 L'obligation de déclaration des éléments essentiels caractéristiques du traitement prévue par l'article 17 de la loi de 1992 et son corollaire à savoir l'inscription dans un registre public organisée par l'article 18 ne s'appliquent pas aux traitements visées par l'article 20 de la même loi, c'est à dire « *lorsqu'un système spécifique d'autorisations ou de déclarations préalables de traitements prévoyant la mise à disposition d'un comité de surveillance particulier des informations visées à l'article 17... et l'inscription dans un registre public des informations visées à l'article 17, est prévu par ou en vertu de la loi, les obligations visées aux articles 17, 18 et 19 sont réputées accomplies lorsque l'ensemble de ces informations est tenu de façon permanente à la disposition de la Commission de protection de la vie privée* ».

Une telle disposition est-elle applicable dans le cas de Phenix ? La loi Phenix n'enjoint pas la mise à disposition de la Commission de protection de la vie privée des informations visées par la loi de 1992 et, dans le contexte du subtil équilibre mis en place par la loi Phenix, il serait étonnant qu'il en soit ainsi. Il serait donc utile que le souci de transparence pour le citoyen qui motive l'obligation de déclaration et l'existence du registre public soit satisfait par ailleurs. Nous avons déjà évoqué l'idée d'un cadastre des traitements qui pourraient être tenu par le Comité de surveillance et serait accessible à toute personne.

135. Ainsi, selon l'article 10 de la loi sur le registre national, chaque autorité publique, organisme public ou privé qui a obtenu l'accès aux informations du registre national ou la communication desdites informations désigne, au sein ou en dehors de son personnel, un consultant en sécurité de l'information et en protection de la vie privée qui remplit entre autres la fonction de préposé à la protection des données visées à l'article 17*bis* de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des données à caractère personnel. L'identité du consultant en sécurité de l'information et en protection de la vie privée est communiquée au comité sectoriel du registre national visé à l'article 15. Cf. également à cet égard, l'article 24 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une banque carrefour de la sécurité sociale, article revu par la loi du 6 août 1993 (cf. également les points 7° et 8° de l'art. 46 de la même loi).

Conclusions

65 L'irruption des exigences de la loi de protection des données à tous les stades de l'organisation et de la vie du pouvoir judiciaire révolutionne nos Palais et oblige à des compromis auxquels le pouvoir judiciaire, réticent au départ, semble s'être soumis. Nombre d'organes ont été créés et leur composition, le partage de leurs compétences illustrent la difficulté de ce compromis. Sans doute, la solution trouvée est, à maints égards, originale et s'écarte des solutions classiquement admises dans les autres administrations. Le comité de surveillance n'est pas un comité sectoriel comme les autres et lorsqu'il s'agit de juger des décisions du comité de gestion, il n'est point question de sortir du cercle de la famille du pouvoir judiciaire.

Il s'agit à présent de voir comment, la loi Phenix désormais en application, les comités de gestion, de surveillance et des utilisateurs nommés, le système va évoluer. Sans doute, la trentaine — le nombre d'arrêtés royaux n'est-il pas en lui même significatif de la difficulté du propos — d'arrêtés royaux mettant en œuvre la loi Phenix et la loi relative à la procédure par voie électronique annoncée pour la fin de l'année répondront à certaines questions que nous nous sommes posées.

Phenix fera probablement ses maladies de jeunesse et il sera nécessaire de réexaminer les lois et arrêtés qui l'encadrent.

66 En ce qui concerne cette fois la conformité de la loi Phenix aux prescrits de la loi dite vie privée, sans doute, l'analyse des finalités révèle-t-elle quelques manques de précisions par rapport aux exigences de détermination et d'explicitation requises par la loi dans la définition des finalités. On apprécie cependant le chemin parcouru depuis l'avant projet jusqu'au texte final,

même s'il faut regretter l'absence, à la Chambre, de débats relatifs à la protection de la vie privée. Sans doute, l'application des dispositions de la loi de 1992 révèlera bien des surprises, en particulier lorsqu'on s'apercevra que les traitements mis en place concernent bien d'autres questions que les dossiers judiciaires et par là bien d'autres personnes que les seules justiciables. Ces personnes réclameront l'accès à leurs données et souhaiteront à juste titre contrôler que l'utilisation généralisée des technologies de l'information et de la communication ne modifie pas de manière subreptice mais certaine l'équilibre des relations entre le justiciable et le pouvoir judiciaire.

À ces risques de dérive, il faudra être attentif : sécurité et transparence des flux au sein du pouvoir judiciaire sont essentielles pour maintenir la confiance des auxiliaires de la Justice et des justiciables en ce dernier recours qu'est la Justice. Gageons que les organes mis en place s'en souviendront l'heure venue.