The belgian case

Poullet, Yves

Published in:
E-justice

Publication date:
2008

Document Version
Publisher's PDF, also known as Version of record

Chapter XII
The Belgian Case:
Phenix or How to Design E-Justice Through Privacy Requirements and in Full Respect of the Separation of Powers

Yves Poullet
University of Namur, Belgium

ABSTRACT

This chapter examines the ambitious Phenix project, a global project for the whole computerization of all Courts and Tribunals in Belgium, with the use of ICT by all stakeholders. It focuses especially on the legislative measures that have been taken, mainly in relation to data protection and legal value of the documents generated by the use of the electronic procedure.

INTRODUCTION

Phenix is the brand name of a project which aims to introduce ICT at all the steps of the judicial procedure in Belgium, no matter the affair engaged in: criminal,[1] civil, commercial, and so forth. In other words, Phenix is a global project for the whole computerization of all courts and tribunals in Belgium. Since the introduction of the dossier until its notification, Phenix aimed to have the actors involved in these different phases: the lawyers, the magistrates, the reg-

istrars, the public prosecutors, and the process servers use the technologies in a secure and efficient way. This very ambitious project has been approved by two legislative acts. The first one, the "Phenix Act," was enacted on August 10, 2005.[2] It institutes the information system called "Phenix," describes its mission, and sets up different organs in order to regulate the system. What is more noticeable in that legislation is the importance given by the legislator to apply and follow strictly the data protection principles in order to build up the Phenix Information System. The second act "relative to the judicial procedure by electronic way" dates from July 10, 2006[3] and aims to modify certain provisions into the Civil and Penal Procedural Code in order to give legal value to the documents generated by the use of the electronic procedure settled up by the Phenix Information System. Our short contribution will analyze these two facets of this legislative input.

Before starting, perhaps a few words about the origin[4] and the present situation of the Phenix Belgian model would be needed. Apart from 1990, certain initiatives were taken in Belgium, but these initiatives were local and not sufficiently coordinated. They were focusing on the internal use by tribunals of computers and the development of certain software aiming to support the tribunal members' work. The concept of a global "e-justice" project has been launched by the previous government in 2000, on the basis of the studies realized by a large consortium,[5] joining together all the stakeholders, and a call for tender has been issued in 2001. Three main concerns explain the launching of a global and strongly centralized project: (1) the development of the Internet which creates an opportunity but also an absolute need to integrate the different databases; (2) the obligation to avoid all the problems raised by the incompatibility between the material used at the different levels; and (3) the idea that such a centralized project will diminish at midterm the costs of the functioning of the tribunals. Several technical working groups[6] have been settled up in order to elaborate and formulate the needed recommendations to address to the legislator, to the furnisher chosen, and definitively to the different actors involved by this revolution. The first concrete works have started in 2002; two acts have been promulgated in order to fix the legal context of the Phenix project, and no less than 18 royal decrees have to be drafted.

Notwithstanding all the efforts of all the actors and the budget afforded to ensure the success of the project, recently in March 2007, the present Ministry of Justice has announced the Phenix project's failure and the obligation to stop the works initiated. It seems that this failure is due to the difficulties met by the supplier to solve complex technical problems. A litigation is in course before a Belgian court between the state and its furnisher. The next government, which will be formed after the next elections in June, will have to decide which follow-up will be given to the project. From this bad Belgian experience, a first conclusion must be drawn: even if we need to have a global project in order to structure all the developments, it is absolutely needed to start with local and dedicated experiences in order to learn apart from these partial experiences how to adapt continuously these developments and to solve the concrete difficulties met at any stages. Another benefit of this experimental approach is also to progressively convince all the stakeholders (the magistrates, the registrars, the process servers, the lawyers, and, finally, the citizens) of the benefits of the project and to hear from them their expectations about such a project. Too much reluctance has been met from different groups, shocked by this managerial revolution imposed without real consultation.

PHENIX: AN ILLUSTRATION OF THE PRINCIPLE "DESIGN BY PRIVACY"[7] AND ABOUT THE DIFFICULTY TO RESPECT THE CONSITUTIONAL PRINCIPLE ABOUT THE SEPARATION OF POWERS

*Article 2 of the 2005 act setting up Phenix is enunciated as follows: "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."("It is settled up an Information system called Phenix, which has for purposes the internal and external communication requested for the Justice needs, the setting up of a case law data base, the working out of statistics and the assistance to the management and administration of judicial institutions")*This provision and the precise enumeration of the different purposes of the Phenix project is illustrative of the importance given by the legislator to follow strictly the first Privacy principle: all processing must be created for legitimate, determinate, and explicit purposes.[8]

The following provisions of the act are describing more precisely these different purposes and implicitly are fixing the recipients of the different processing, the data to be processed, and the duration of the data storage, according to the principle of proportionality: "Data might be processed and kept only if they are necessary for the achievement of the legitimate purpose of the processing."[9] Two examples might be given on that point. Article 7 distinguishes the court decisions databases used for internal purposes and the court decisions databases diffused publicly. As regards the second category, the act imposes the duty to make anonymous the decisions before any diffusion. What is not asked as regards the first category insofar is that the purpose of this second processing ought to support the members of the jurisdiction having issued the decision to "maintain a consistency as regards its jurisprudence," as explained by the Ministry of Justice. Another example definitively is the use of certain data for statistical purposes (art. 10 and ff), which might help internally to support decisions about the management of the tribunals, but might never be used for controlling the work achieved by each judge individually.

This concern to follow the privacy requirements explains also the importance given to the security of the different processing. This obligation to have secure processing must be the object of different royal decrees, and certain norms might be imposed at that point. This obligation raises certain problems. So, as regards the access to the different files opened at a court, it has been foreseen that the access will be open to all the members of the Bar Association. The control of the identity and the quality of the requester will be ensured as regards the first point by the use of a secure authentication and, as regards the second, by the fact that the requester belongs to the lists held by the different Bar Associations under the basis of his or her national registration number. This checking method has raised difficulties. Certain lawyers have refused to give their national registration number to the Bar Association and have raised privacy concerns about the obligation to use their electronic identity card as a unique way of authentication, arguing that they would like to distinguish clearly the authentication method they are using in the context of, from one part, their professional activities and, from the other part, as citizens.[10]

Another more crucial problem was the control of the legitimate interest of the requester

to have access to the different files.[11] Finally, the system proposed was the possibility for the lawyer in charge of the file to know through the login of all the access to control *a posteriori* the names of the colleagues which have access to the files. It is not obvious that this system will be sufficient to avoid any abuse.

Other questions about the application of the data protection have to be mentioned. Particularly, it has been pointed out that the right of the data subjects must be respected by the data controller. Data subjects are of various natures: definitively, it concerns all the citizens which are concerned by the litigation directly (the plaintiff and the assignee) but also indirectly (a person quoted by the judge, a witness), it might be also the advocates and the judges. So the question is: to what extent the present provision included in our civil or penal procedural codes enacting a limited right of access are complying with the data protection legislative requirements about the right to be informed, the right to get access, and the right to correct or delete certain data? This question is still discussed.[12]

The main problem met by the legislator by setting up the Phenix information system surely was the choice of the different organs to be installed in order to manage and to rule the development of this information system. Three main concerns have to be taken into consideration. The first one was to respect the holy and constitutional principle of the separation of powers, particularly the split between the executive power and the judicial one. The second addresses the delicate question of the data protection and again the question of separation of powers between the legislative power represented by the Data Protection Authority (the Belgian Commission pour la protection de la vie privée) and the judicial one. How do we ensure the compliance of the Phenix development with the data protection requirements? Finally the third one is to ensure that the information system meets the needs of the different stakeholders involved.

To answer to these concerns, the Phenix Act puts into place three organs: the "Management Committee" (Comité de gestion), the "Surveillance Committee," and, finally, the "Users' Committee." The main competence of the first one is to ensure the daily management of Phenix and to take all initiatives which will contribute to its efficiency. The committee has therefore the possibility to decide on different aspects like technical agreements, conformity certificates as regards the legal value of certain electronic documents, and to establish control and security mechanisms.[13] It proposes to the Ministry the draft of the royal decrees needed for the implementation of the legislative texts. An annual report about the committee's activities must be established for the Highest Court of Justice (Cour de cassation) and the Ministry of Justice. Furthermore, the committee has to intervene in case of technical deficiencies or nonrespect of the Phenix rules. The committee's composition reflects the duality of nature of the Phenix system belonging both to the executive power and to the judicial one. Twelve members nominated by the King are composing the committee, 6 under proposal by the judicial power, and 6 under the proposal of the Ministry of Justice.

The "Surveillance Committee" is established by the Phenix Act as a sectoral Data Protection Authority established within the Belgian Data Protection Authority but having a lot of autonomy and no subject to control by its mother institution.[14] Furthermore, the committee examines the complaints introduced as regards the nonrespect of the data protection provisions and might introduce any proposals about all questions relative to privacy requirements applied to the Phenix information system and its evolution. The composition of this committee has been subject to a lot of discussion between the judicial power and the Data Protection Commission.[15]

The judicial power in a first moment rejected any form of interference by the Data Protection Authority, accepting only the presence of a member of the Data Protection Authority and only with consultative voice. Finally, the compromise proposed by the government and taken again by the act was to have a committee with six members, three chosen by the DPA and the three others nominated by the parliament amongst the magistrates. The chairman necessarily must be a magistrate.

The last organ to be put into place is the "User's Committee," in charge of proposing to the Management Committee any initiative in order to promote the Phenix use. The committee joins together 24 members representing all the stakeholders but with a huge majority of magistrates (16/24). It illustrates once again the fear expressed during all the discussion by the magistrates about the risk of losing their independence in the same time information systems were introduced in their office.

PHENIX: HOW TO GIVE LEGAL VALUE TO ELECTRONIC PROCEDURAL DOCUMENTS[16]

The introduction of the electronic file definitively is the major revolution introduced by the 2006 Act relative to the procedure by electronic way. Three main principles are asserted: the first one is the freedom for everybody to choose or not the electronic procedure: "*Sauf dispositions légals contraires, personne ne peut être constraint de poser des actes de procédure ou de recevoir des documents relatifs à des actes de procedure par voie électronique.*"[17] This consent's principle[18] is however alleviated by the possibility to impose the use of the electronic procedure to certain professions by royal decree. In order to ensure the real consent of the actors to use the electronic procedure but also the opposability of the electronic exchanges, a list of the actors, professional or not, who do accept the new tools to communicate in the context of the procedure will be held and published by the Ministry of Justice or by the professional associations. The consent might be withdrawn. Precisely the use of an electronic judiciary address is left to the free choice of the persons. The electronic address is defined under Art. 6 of the 2006 Act, as : "*l'adresse de courier électronique, attribuée par un greffe et à laquelle une personne a accepté, selon les modalités fixées par le Roi, que liui soient adressées les significations, notifications et les communications.*"

The second principle is the equivalency principle. Under this principle, the electronic address is equivalent to a physical address and has the same permanency as the traditional one. Furthermore, it must be considered that all the electronic documents generated in the context of the procedure are assimilated as regards its legal value to a paper document and that electronic signature in that context have the same legal value than the traditional handwritten signature. As Montero[19] pinpointed, it must be clear that under the 2006 Act, only advanced or under the Belgian terminology qualified signatures complying with the EU Directive requirements are recognized in the context of the e-justice system and not all electronic signatures[20] in order to ensure an easier legal security. Finally, one pinpoints the principle of the unity of the electronic file insofar as the electronic nature of the file; it is no more necessary to distinguish copies and original, insofar this latter might be reproduced in a nonlimited way.

As regards the relationships with the third parties, essentially meaning the lawyers and the process servers, the idea is to authorize either the downloading of the files or certain pieces of the procedure either their access, through the Judiciary order's portal, only after a double

checking: first, the requester of the access needs to be identified through a secure authentication; second, the system will seamlessly check near the appropriate databases held by the professional associations, his or her quality. It is quite obvious that the Phenix system will support all types of documents (open office, XML, PDF, etc.). Finally, the act contains certain provisions about the consequences of a not guilty[21] dysfunction of the information system (virus, breakdown of the information system, etc.) which are assimilated[22] to Acts of God "*when that dysfunctioning hinders the exercise of the citizen's rights.*" Let us now have a look at the different steps of the procedure.

The introduction of a litigation before a court (la mise au rôle) would have to be, apart from now, realized by an electronic message.[23] On that point, it might be remembered that the role is held through electronic means publicly accessible, but any access is registered in order to avoid abuses as regards the privacy protection requirements.[24] The registrar automatically attributes to the affair a specific identifying number which will follow the case during its entire judicial life (including in appeal or before the highest Court of Justice). This identifying number contains neither the name of the parties, nor other personal data. The registrar is in charge of making the inventories of the files. Certain norms as regards the preservation of the integrity of the pieces notwithstanding the change into the technology must be defined.

As regards now the management of the file, the Phenix Information system will receive the additional elements appropriate to each step of the judicial procedure: "*Toute autre communication par pli simple ou recommandé peut avoir lieu valablement par voie électronique ou par introduction dans le système Phenix.*"[25] The article 9 of the 2006 Act determines the moment of the delivery of the electronic document as follows: "*la délivrance d'un document électronique est le moment où le destinataire peut prendre connaissance du contenu de celui-ci.*" In order to avoid any litigation as regards this moment, it is possible to make recourse to a third party. In that case, the moment of the delivery is fixed by the statement given by this third party certifying the delivery of the message to the recipient.

The fixation of the audience must also be done through electronic messages. The judgment will be issued and signed electronically by the judge before it is sent to the database, the internal one, and after having been duly made anonymous by the Registrar, the publicly accessible one.

Two peculiar operations must be analyzed additionally, the "*signification*" and the "*notification.*" Both operations are aiming to make the citizen or his/her lawyer aware of the existence of the pursuit or of the judgment. For ensuring these two operations, the use of an electronic message is possible[26] through the intervention of a trusted third party who will have to ensure that the document has been delivered without modification (certificate of integrity) to the electronic address of the addressee and that this delivery has taken place at a precise moment (time stamping). For achieving it, the 2006 Act foresees the intervention of a "communication service provider"[27] who will certify the delivery and the moment of this delivery.[28] To be complete, it must be noted that the legislation puts in place a hybrid system in case the final recipient has no electronic address. In that case, the service communication provider will make a copy on a paper certified conform of the message and deliver it to the process server who will deliver the document following the traditional way.

CONCLUSION

Is there a Belgian Phenix model? In my opinion, it would be too easy to simply answer by the negative, invoking the present failure of the Phenix launching. It is obvious that the promoters have been too ambitious and, perhaps, a more progressive approach associated with the actors, especially magistrates, registrars, and lawyers, step by step, working on specific domain and using pilot experiences would have been better. Notwithstanding these facts, one would like to underline the qualities of the legal framework put into place to ensure e-justice, which might be in my opinion viewed as a model for foreign countries. So we might consider that the Belgian legislator, even if the solutions are not always perfect, has designed a privacy compliant system and that, through the organs settled up, the independence of the judiciary power vis-à-vis the executive power is safeguarded.

FUTURE TRENDS

Two points have to be considered as crucial in the future. First, since through a global information systems at the hands of the magistrates their informational power is increasing by their possibility to cross a certain number of information about the parties, it must be feared that the principle of the "equality of the weapons" would not be respected. In that respect, data protection requirements are important. At the same time, the fact that the information system is operated and sometimes developed by the administration put at risk in the long term a progressive loss of the independence of the judges. The solution proposed by the Belgian legislation is in that perspective notice worthy even if they appear a bit intricate and too complex as regards the day to day management.

As regards the modifications introduced by the legislator into the civil procedural code, we might subscribe to the main principles asserted through the multiple provisions: the consent permits to avoid any risk of discrimination between those who adopt the new electronic system and the others more reluctant to it. The "functional equivalency" principle has permitted to introduce concept like electronic address, electronic file, electronic signature, electronic signification, and notification. By doing that and by proposing a real secure communication system with the intervention of trusted third parties, control of access, double checking, and so forth, the Belgian legislator proposes to the other European legislator a really attractive model.

REFERENCES

Burton, C., & Poullet, Y. (2005). A propos de l'avis n°9/2005 de la Commission de protection de la vie privée du 15 juin 2005 sur l'encadrement des listes noires. *RTDI, 23*, 100 and ff.

Colson, B., Montero, E., & Mougenot, D. (2007). *Phenix - les tribunaux à l'ère électronique: Actes du colloque du 8 Février 2007.* Cahiers du Centre de recherches informatique et droit, 29. Namur: Crid, Facultés universitaires Notre-Dame de la Paix de Namur.

Danieli, F. (2006). L'application de la loi vie privée au pouvoir judiciaire et au secteur policier: Disaster or much ado about nothing. *RDTI, 25*, 169-203.

Henrotte, J. F. (Ed.). (2005). *Phenix et la procédure électronique.* Bruxelles: Larcier.

Henrotte, J. F., & Poullet, Y. (Ed.). (2005). *Cabinets d'avocats et technologies de l'information.* Bruxelles: Bruylant.

Hubin, J., (2005). Les relations Barreau-Palais: la diffusion des données jurisprudentielles dans le cadre du programme « Phénix » d'informatisation de l'ordre judiciaire. In J. F. Henrotte & Y. Poullet (Eds.), *Cabinets d'avocats et technologies de l'information.* Bruxelles: Bruylant.

Lamberts, V. (2007). La signification par voie électronique. In B. Colson et al. (Eds.), *Phenix: les tribunaux à l'ère de* l'électronique. Bruxelles: Bruylant.

Montero, E. (2007). Signature et preuve des envois dans le cadre des communications judiciaires électroniques. In B. Colson et al. (Eds.), *Phenix: les tribunaux à l'ère de l'électronique.* Bruxelles: Bruylant.

Mougenot, D. (2007). Le code judiciaire à l'épreuve du cyberspace: une réforme réussie. In B. Colson et al. (Eds.), *Phenix: les tribunaux à l'ère de l'électronique.* Bruxelles: Bruylant.

Poullet, Y., & Moreau, D. (2006). La justice au risque de la vie privée. In J. F. Henrotte (Ed.), *Phenix et la procédure électronique.* Bruxelles: Larcier.

Vandermeersch D. (2007). Phenix à l'épreuve de la procedure pénale. In B. Colson et al. (Eds.), *Phenix: les tribunaux à l'ère de l'électronique.* Bruxelles: Bruylant.

ENDNOTES

The specific legislative provisions about the criminal procedure will not be commented in the present contribution. About these provisions, read Vandermeersch (2007).

2 As regards this first act and its analysis, see Henrotte (2005) and Henrotte and Poullet (2005). This act has been published at the Belgian Official (Moniteur Belge) (loi du 10 août instituant le système d'information Phenix, M.B., 1er septembre 2005, p. 38.305).

As regards this second act and its analysis, see the various contributions published in Colson et al. (2007). No less than 24 royal decrees were foreseen as regards the implementation of both acts. Some of them have been already drafted but not yet submitted to the royal signature. This Act has been published at the Belgian Official Journal (Moniteur Belge) (Loi du 10 juillet 2006 relative à la procédure par voie électronique et du 5 août 2006 modifiant certaines dispositions du code judiciare en vue de la procédure par voie électronique, M.B., 7 septmebre 20006, p. 45517).

4 About this genesis, see Hubin (2005).

5 The consortium "e-Justice" has been created by the Ministry of Justice in 2002 and 2003 under the direction of three university professors: G.de Leval (ULG), P. Taelman (U. Gent), and Y. Poullet (U. Namur). It has worked during 18 months and produced reports which have been taken as points of reference by the authors of the project, put under the leadership of President Verougstraete. First, president of the Cour de Cassation (the highest Belgian Court of Justice). About these works, the reports published at the CRID's Web site: http://www. crid.be

11 technical groups have been therefore created. The most important was the Juricontrol W.G. in charge to formulate the legislative provisions about the Phenix system. Others groups have also to be quoted: "Security," "Modelisation," "Change Management," "Communication," "Nomenclatures and Codes," "Legal value of electronic judicial documents," "Archives," "Infrastructure," "Software Applications," and "External relationships with process servers, lawyers, and so forth."

On that point, see (Poullet and Moreau, 2006)

The recitals of the act refers explicitly on that point to the famous Rotaru Case decided by the European Human Rights Court of Justice (EHRCJ) May 4 and published notably in 2001. *Rev. Trim des droits de l'homme*, 2001, p. 137 and ff, with annotations by O. de Schutter). This decision recalls these principles directly derived from the article 8 of the European Convention of Human Rights. As regards the EU Directive 95/46 on Data Protection (OJ., n°L.281, 23th of Nov., pp. 31 and ff), the same principles are enunciated by art. 6.1 b.

See as regards this principle, art. 6 c and e of the EU Directive 95/46 quoted footnote 8.

The Belgian Privacy Commission argued in the same sense in its opinion delivered May 24th, 2006 about "Identification and electronic signature within the Phenix I.S." On that opinion, see the Web site of The Belgian Privacy Commission: http://www.privacycommission.be

11 By example, one might imagine that a lawyer defending a citizen against his neighbour for vicinity questions will access different files including criminal files of this neighbour in order to argue against him.

12 On that point, see Danieli (2006).

13 Appeals against the committee's decisions are foreseen before the Highest Court of Justice (Cour de cassation). Once again, the existence of this recourse put into evidence the intent of the Belgian legislator to maintain the independence of the judiciary power by giving to it the last word.

14 On that point, see the explanation given by the Ministry of Justice: "*Par ailleurs, autoriser la Commission de 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 (dépendant du législatif) et l'Ordre judiciaire, tous deux institutionnellement et légalement indépendants.*" (*Doc.Parl. Ch.*, 2004-2005, 1654/001, p. 42).

15 See the opinion delivered by the Belgian Data Protection Authority (Opinion n° 11/2004 (Poullet & Moreau, 2006), point 22, published on the Web site of the Belgian Privacy Commission).

16 In that point II, we will analyze only the question related to the civil procedure. The additional problems raised by the electronic criminal procedure are too complex for being evoked here. See Vandermeersch (2007) about these additional problems.

17 Art. 4 of the 2006 Act recalling the same principle already asserted by the art. 4 §1 of the act on electronic signature.

18 About this fundamental principle, see Lamberts (2007).

19 Montero (2007).

20 "*Chaque fois qu'une disposition légale prévoit la signature d'une pièce de la procédure et qu'il s'agit d'une pièce électronique, celle-ci est pourvue d'une signature qualifiée... Cette signature électronique qualifiée est assimilée à une signature électronique. .. La signature qualifiée s'entend de la signature électronique avancée définie à l'article 2, 2° de la loi du 9 juillet 2001 fixant certaines règles relative aux cadres juridiques pour les signatures électroniques et les services de certification, certifié par un certificat qualifié visé à l'article , 4°, de cette loi et créé avec un dispositif sécurisé au sens de l'article 2, 7° de cette loi.*" (Art. 7 of the 2006 Act). To be complete, it has to be underlined that the electronic signature linked with the use of the electronic identity card definitively is a "qualified" signature

and thus might be used in order to sign any electronic document of the procedure. What does "not guilty" mean? Is any lawyer who participates in the Phenix system obliged to use a antivirus system and if yes with which quality? On that question, see Mougenot (2007).

22 Art. 9 §2 of the 2006 Act.

23 As it is foreseen apart from now under the revised Art. 713 of the Civil Procedural Code: "*le role est créé et conservé d'une manière qui rende possible sa consultation et garantit sa lisibilité.*"

24 So certain companies were noting systematically the names of certain litigants (employees suiting their employers, bad payers, etc.) in order to constitute black lists. About this phenomenon, see Burton and Poullet (2005).

25 Art. 4 of the 2006 Act.

26 Art. 6 of the 2006 Act. "*Sans préjudice des conventions internationales en la matière, la signification peut avoir lieu par voie électronique. Elle a lieu à l'adresse judiciaire électronique par l'intermédiaire d'un prestataire de service de communication...*"

27 Art 10 of the 2006 Act. This article foresees a certain number of requirements to be observed by the communication service provider. The compliance with these requirements is verified in the context of a licensing procedure quite similar to the licensing procedure used for the certification service providers in case of electronic signature.

28 This actor might be considered as a Trusted Third Party, combining two functions, that is, the time stamping function and the evidence of the sending and receipt of the messages.