Acta chir belg, 2002, **102**, 420-426

The Protection of the Patient's Private Life : the Computer Challenge Second part (1)

M. Van Overstraeten, Luc Michel***

*Aspirant du F.N.R.S., Département de droit public de l'U.C.L., Louvain-la-Neuve, Belgium ; **Service de Chirurgie, Cliniques Universitaires U.C.L. de Mont-Godinne, Yvoir, Belgium.

Key words. Bioethics ; privacy ; confidentiality ; medical secret ; computer science.

Abstract. Today, medical practice is invaded by a growing number of technologies of all kinds, among which computer techniques have an important place. Although they have significant advantages, for instance in terms of medical record management, they give rise to several problems, particularly concerning the confidentiality of the patient's data with regards to third party. A great number of specific provisions, complementary to the general texts protecting private life (examined in the first part of this two parts article), endeavour to solve these problems. It is true that these provisions are recent, have various origins and often appear as rules difficult to understand. Yet, they are partially inspired by a common logic. Relying on these common features, the authors make two suggestions for the future, in order to avoid that the growing computerisation of medical practice eventually destabilises the health care relationship :

a) Any *dictatorship of confidentiality* must be rejected
b) Stimulating a sense of *professionalism* is most likely the way to avoid an anarchic and unrealistic development of rules aimed at regulating the health care relationship.

The rules protecting the patient's private life form a vast whole. A first analysis has highlighted the structure and the characteristics of this whole (1). The backdrop of this analysis was the traditional model of the doctor-patient relationship. However, neither the deep changes nor the interferences of all kinds affecting this relationship today can be ignored. These are due to the invasion of medical practice by a growing number of technologies. Among these, the computer techniques, of which the impact on the patient's private life is far from being insignificant, have an important place. This is why this article goes deeper into the analysis of this issue. After giving a summarised description of the forms and consequences of the computer phenomenon in medicine, this article mentions a series of rules aimed at dealing with it at the level of private life. Then, it goes on to examine the specificities of these rules, which leads to make a few observations to be used as beacons for the future. This article should be read in the light of Part One (2).

I. The computerisation of medical practice

In the medical sector, invoicing was the first concerned by the development of the computer technologies. Computerisation then extended to clinical databases. Today it is about to revolutionise the management of medical records. Application programs are being designed to computerise the management of these records. Networks are being set up to interconnect them. Databases, both internal and external to the health care structures, are being created in order to centralise the data of the medical records anonymously. This evolution is not over. Other developments in computer science are about to change the doctor-patient dialogue dramatically. The patient will be able to send information relating to his or her health status electronically and receive advice from the physician electronically as well, while multimedia encyclopaedias will be connected to the personal medical data in order to make them more accessible to the lay person (3,4,5).

These developments have already brought and will continue to bring significant improvement in the health care sector. The large-scale computerisation of the medical records, in particular, will allow additional data to be included into these records, which in turn will improve the follow-up of the patient. It will ease the exchange of data between hospitals and primary care structures. It will make the comparison of patients easier, for instance in the context of studies on tolerance to

(1) The First part "The Protection of the patient's Private Life/ a Vast Normative Landscape" has been published in the previous issue, Acta Chirurgica Belgica 2002, 102, 5 : 282-288.

drugs. Or it will allow the authorities and the profession to collect a great number of essential data more easily. As for the use of electronic communication between physicians and patients, it will improve the information that the patient receives on his or her health status as well as his or her ability to understand this information ; it will allow him or her to give a fully informed consent to the care that the practitioner proposes to give (6,7).

However, the computerisation of medical practice gives rise to difficulties.

The purchase of computer equipment and the training necessary in order to use it generate high costs. There is a danger of discrimination between professionals or structures that can afford it and those who can not. Moreover, the medical sector is experiencing the development of a vast number of application programs intended, among others, to manage the medical records. Not all of these programs are compatible with each other. Other difficulties are associated with these general problems : how to set up an effective standardised structure for the electronic medical records ? How can the patient's and the physician's freedom of choice be preserved, since the medical records have to be centralised by a given practitioner (8, 9, 10) ?

At the level of private life, the use of computers could bring the patient to use the *freedom* he or she has in his or her private realm in an improper way. Indeed, if access to the medical records becomes commonplace and if the patient is given the keys in order to understand the medical science, he or she could become suspicious of the medical acts proposed by the physician. This could bring him or her to reject the suggested treatment if it does not meet his or her expectations. This could eventually weaken the doctor-patient relationship.

The threats hanging over the *confidentiality* of the patient's private life are even more worrying, especially those relating to the *confidentiality* of his or her data with regards to third people. Two examples are enough to demonstrate the extent of the problem. On the one hand, computerisation of personal data leads most of time to the connection of these data to a computer network. Therefore, one can fear that clever hackers take control of them with complete impunity, be it to satisfy their personal interests (curiosity, perversity, revenge, financial gain, etc.) or the interests of unscrupulous employers, insurers or next of kin. On the other hand, the computer coding of the patient's medical data allow them to be put in relation with computer data of different origin, among other for commercial purposes. One just has to think about the case of this American bank that required the immediate reimbursement of debts from certain customers after it managed to learn that they had cancer (11). In this case as in the other, the violation of confidentiality will have consequences all the more significant since computer technologies make possible the storage of a great number of personal data in one single place.

The following fact cannot be ignored : computers dramatically increase the risks of violation of information relating to the patient's privacy. They make this information more accessible, hence more vulnerable. If not controlled properly they constitute an unprecedented danger for its confidentiality, the very pillar of the doctor-patient relationship. The use of computers could lead to medical watch, and even to an unequalled supervision of the individuals' private lives (12). This would have serious consequences on the quality and the effectiveness of the health care relationship. The patient would, consciously or not, modify his or her behaviour, either by not requiring treatment, or by concealing his or her identity, or by choosing the information he or she gives to the physician, or perhaps even by accepting to pay a high price to have access to hospitals that are not connected to the general computer network. He or she would also be tempted to turn to alternative, unconventional forms of health care (13).

II. Numerous provisions

In terms of the protection of private life, computers represent a real challenge to the health care world. How is this challenge taken up at the normative level ? There is no lack of texts. Rules mentioned in Part One and aimed at guaranteeing the private life of the citizen in general, and of the patient in particular also apply here. They are supplemented by several specific provisions ensuing from the growing computerisation of society and medical practice. This second category of rules is now going to be examined briefly.

First of all, there is a series of provisions, of state origin, aiming at controlling the automatic processing of personal data, irrespective of the sector in which it is implemented. These general texts apply to electronic records or other electronic databases used in the medical sector, from the moment they imply any automatic processing of personal data.

Some provisions were drawn up at the international level. For instance, the Council of Europe has the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed in Strasbourg on 28th January 1981. The European Union has Directive 95/46/CE of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data (14).

Other texts have been adopted at the national level. In the Belgian legal order, it is the Act of 8 December 1992 on the protection of private life with regards to the processing of personal data (15,16). This Act, elaborated in

connection with the Convention of the Council of Europe and adapted in 1998 in order to transpose the European Directive (17), particularly concerns the fully or partially automated personal data processing (art. 3, § 1) (18). It makes provision for a series of measures aimed at guaranteeing the protection of the freedoms and fundamental rights of the natural persons concerned and particularly the protection of their private life (art. 2).

Some of these measures contribute to the respect of the *confidentiality* of the patient's private life. First of all a particular scheme specifically applies to the processing of data regarded as sensitive, among which appear those a patient is likely to confide to his or her physician. The Article 7 of the Act regulates the processing of health-related data. It is prohibited in principle (art. 7, § 1) but accepted in certain cases (art. 7, § 2), among others when it is necessary "for the purposes of preventive medicine, of medical diagnoses, of the administering of care or treatment, either to the person concerned or to a relative, or for the purposes of the management of health services acting in the interest of the person concerned" (art. 7, § 2, j). In these cases the processing of these data has to respect specific conditions. Some of these conditions are laid down by Article 7 itself — the processing has to be done under the responsibility of a health care professional bound by secrecy, just as his or her employees or representatives. (art. 7, § 4) (19). But the same Article also entrusts the Government with task of determining other conditions (art. 7, § 3) (20). As for Article 6, it provides for a similar scheme for personal data relating, among others, to sexual life and religious or philosophical beliefs and processed for medical purposes or for the purposes of the management of health services (art.6, § 2, j). Then, at a more technical level, rules see to guaranteeing the security of data processing (art. 16). Theses rules apply to the processing of the above-mentioned sensitive data as well as to the processing of other data referred to in the Act. They are binding for people responsible for the processing as well as for their subcontractors.

The Act of 8 December 1992 also provides for measures aimed at giving concrete expression to the *freedom* of the patient's private life. Anyone concerned by a data processing falling within the scope of the Act is granted certain rights aimed at giving him or her control over his or her personal data : the right to obtain the communication of the health-related data to be processed, either directly or through a health care professional (art. 10, § 2), the right to correction of the incorrect personal data (art. 12, § 1, al. 1), the right to oppose to the processing of his or her personal data, provided he or she has a serious and legitimate reason to do so (art.12, § 1, al. 2), the right to obtain the deletion or to forbid the use of any personal data that, given the aim of the processing, is incomplete or irrelevant, of which the recording, the communication or the storage is forbidden, or that has been stored beyond the authorised period (art.12, § 1, al. 5).

Provisions *peculiar to the medical sector* also have to be taken into consideration.

At the international level, the Committee of Ministers of the Council of Europe adopted a recommendation on regulations for automated medical data banks (Recommendation R (81) 1 of 23 January 1981) and a recommendation on the protection of medical data (Recommendation R (97) 5 of 13 February 1997). The latter is more detailed and replaces the former. It suggests that the States take appropriate measures in order to guarantee the respect of fundamental rights and freedoms, including the right to private life, during the collection and automated processing of data "concerning the health", having a clear and close link with health, or genetic data. (art. 1, 2, et 3). To that effect, it proposes measures similar to those laid down in the above-examined general provisions : the specifying of the purposes for which data can be collected ; the determination of the conditions and security measures to be respected within the context of the data processing, the granting of prerogatives to the person concerned, so that he or she has a right to inspection of the processed data.

At the national level provisions specific to health-related electronic data are gradually adopted. In Belgium, these provisions still lack certain cohesion. Article 45bis of Royal Decree n° 78 of 10 November 1967 on the practising of the art of curing — an article inserted in 1999 (21) — allows the Government to lay down, on the advice of a multidisciplinary workgroup, the minimal criteria to be met by application programs designed to manage the electronic medical and nursing records in order for them to be approved by the Public Health Secretary. The Royal Decree of 3rd May 1999 laying down the minimal general conditions to be met by the medical records as defined in Article 15 of the Hospital Act, co-ordinated on 7th August 1987 (22), authorises the electronic storage and management of these records, provided that the conditions otherwise laid down are respected, including the patient's right to be informed about his or her personal data. Moreover, it allows the Public Health Secretary to lay down "practical details for the exchange of data from the records" (art. 1, § 2). Another Royal Decree of May 3rd, 1999 (23) sets up a Commission "Standards in terms of telematics at the service of the health care sector" responsible for giving technical advice in that field (art. 1), particularly in order to promote the electronic exchange of data in the health care sector and the use of patient-focussed electronic records (art.2, § 1). In this last case, the concern to protect private life appears in an express way : the Report to the Government preceding the Decree states that the Commission intervenes in a

context in which it is essential to "implement the precautions relating to the regulation on private life and give the patients the guarantee of a confidential processing of their medical data" (24).

Professional provisions add to these texts of *state* origin. At the international level, the World Medical Association issued a Statement on the Use of Computer in Medicine, which recommends taking various measures in order to guarantee the security and confidentiality of the patient-related data. As for the European Guide of medical ethics it states, following on provisions dedicated to professional secret, principles specifically relating to electronic medical databases (art. 9) : "Physicians shall not collaborate to the setting up of medical databases jeopardising or weakening the patient's right to privacy, to security and to the protection of private life. Any electronic medical database should be put under the ethical supervision of a physician designated by name. Medical databases must not have any link with other databases". In Belgium, many opinions and recommendations issued by the National Medical Order deal with the difficulties arising from the use of computers in medicine, particularly with regards to professional secret (25).

III. Specific provisions

The computerisation of medical data has given rise to its own rules in terms of the protection of private life. Two factors make the reading of these rules difficult. On the one hand, as previously highlighted, they cannot be isolated from the general provisions guaranteeing the protection of the patient's private life. On the other hand, they turn out to be difficult to understand, sometimes even obscure. Within the limited scope of this paper, it is not possible to give all the necessary clarifications. However, as was the case in Part One, this paper tries to highlight some of their essential characteristics, so as to make appear the dynamics that lies behind them. To that effect, the three criteria previously used — time of elaboration, authors, and content of the provisions — are also applied here.

1. *The time of elaboration of the provisions*

Whereas the origins of the rules relating to the medical secret date back to almost twenty-five centuries, texts relating to the protection of private life within the context of medical data processing are not more than three decades of age. In the Belgian legal order, the very oldest date back to the nineties. This can be easily explained by one fact that barley needs reminding, i.e. the problems that these provisions try to solve are new. Computer technologies are a new phenomenon in medical practice.

Moreover, the normative evolution that this makes necessary is not completed yet : certain aspects of this material still have to be dealt with ; the first tendencies have to be confirmed. This just means that the material is still under construction. This is one of the latest stages of the *diversification* process characterising the rules relating to the protection of the patient's private life (26).

This calls for cautiousness. Today's observations are partial and inevitably provisional. They will have to be reconsidered regularly, in the light of the further provisions adopted.

2. *The author of the provisions*

Skimming over the current normative system shows that the texts already adopted have very different origins : there are state and professional texts, national and international. As just said, the material is under construction, but most of the authorities concerned have already mobilised, to various extents, to deal with it.

Moreover, the configuration of these provisions is very close, at least today, to that of rules relating to the respect of private life in general, i.e. complex but not void of effectiveness (27). They seem, for instance, to form a "set of mirrors" as well. They reinforce each other. To take only one example, the Convention of the Council of Europe for the Protection of Individual Rights with regards to Automatic Processing of Personal Data on the one hand, and the corresponding European Directive on the other hand, find in the now-amended Belgian Act of 8 December 1992 the necessary measures specifying their content and giving them effect in the Belgian legal order, while giving the Act a legitimacy and an effectiveness greater than that an isolated national provision would have.

One specificity needs to be highlighted. It relates to the setting up of work groups and other commissions to work along with the normative authorities concerned by the problems arising from medical data processing. For Belgium, for instance, the Commission "Standards in terms of telematics at the service of the health care sector" has been mentioned. These commissions and work groups are advisory organs made up of specialists in the field of computers and entitled to inform the authorities about the inescapable technical aspects. If not used properly, this method could turn out to be problematic. Scrupulous authorities might be tempted to dissect these opinions in minute details in order to get all the ins and outs of the question, thus making the time of elaboration of the rules significantly longer. As for authorities concerned by rapidity and effectiveness, they could be tempted to leave it up to the experts, with a risk of jeopardising the democratic nature of the decision process. Both directions are just as questionable. However, the right balance is difficult to reach.

3. *The content of the provisions*

Numerous remarks can be made on the content of the relevant texts. Within the scope of this paper, only a few general observations will be made.

One of the common characteristics of the provisions mentioned above is their denseness. They try to encompass all the various situations. They multiply exceptions. They give technical details. In short, the more complex they are, the less clear they become.

However, they seem to be guided by three concerns, the same concerns inspiring the texts in preparation. The first concern is to make *basic choices*. They have to determine who can have access to the electronic medical data, i.e. on the one hand the people allowed to process and on the other hand people allowed to consult them. They also have to indicate the purposes for which these people are allowed to have access to the data, and therefore, the period for which access is open. Moreover, they have to specify which data can be processed and consulted. The second concern is to make provision for *technical measures* in order to put these basic choices into practice. These are the measures ensuring the security of data storage, consulting and transmission, as well as the physical protection and the supervision of the computer equipment. It is the field of passwords, access codes, ciphering and deciphering, in other words : the field of cryptology. The third and last concern is to introduce the *reliability standards* that the technical processes have to comply with. They relate, among others, to the minimal conditions that these processes have to meet, determined in the light of the recommendations of the above-mentioned work groups, and to their approval by the authorities (28).

The basic choices are logically in line with the options on which the general provisions protecting the patient's private life are based. On the one hand, they show a concern to guarantee the confidentiality of the electronic medical data. On the other hand, they echo, if not anticipate, within the computer context, choices made at the level of the patient's freedom in his or her private realm. In short, the general texts and those dealing with the computerisation of medical practice show a common inspiration. This is true to the point that provisions can be found in the latter, that just reaffirm principles stated in the former, insisting in this way on their importance in a context where the confidentiality of personal data turns out to be shakier than ever. They strongly underline the right of everyone to respect for his or her private life during the processing of his or her medical data ; they reassert the obligation for secret incumbent upon the health care professionals in charge of this processing (29). Precisely as a result of their common inspiration, rules making basic choices should evolve in the wake of the general rules protecting the patient's private life, unless real or pretended "insuperable technical obstacles" appear, that could prevent the transposition of these general choices into the computer sector. In this case, they should only undergo gradual changes.

As for technical provisions, they are typical for the standards arising from the computerisation of society and medical practice. Most of the time, they attempt to give effect to the protection of the confidentiality of medical data. Given the rapidity of technical innovations, they are bound, contrary to provisions assuming basic choices, to be continuously adapted, either slightly adjusted or deeply amended. This is the price to pay for the security of processing and the reliability of the computer equipment. This is not a small challenge, all the more since the exchange of data requires the compatibility of the systems in a territorial scope as large as possible, ideally at the international level. Can it be reasonably conceived that rules elaborated at this level, and of which the adoption often requires unanimity, are continuously re-evaluated according to technological progress ? This is a thorny problem. Some might be wrongly tempted to question the procedures governing the elaboration of these rules, particularly the legal rules, putting forward the fact that they can barely keep up the pace of this progress.

It should be noted that provisions specific to electronic data, be they technical or not, not only concern the physician. Given the appearance of a "middleman", the computer, at the heart of the doctor-patient relationship, the physician is no longer alone in front of the patient and the data he or she has to process. More and more outsiders have to take part in the health care relationship, be they designers of medical application programs or subcontractors in charge of the management of medical data bases. One is witnessing an *opening* of this relationship, appearing at the same time as the collectivisation of medical practice. These outsiders have to respect certain rules that go as far as to impose on them constraints that, for the sake of the confidentiality of the patient's private life, only physicians and health care professionals have to respect in the traditional context of the health care relationship. There is for instance the obligation to respect a certain form of medical secret or to take concrete measures in order to protect the data against any indiscretion.

IV. Beacons for the future

The intrusion of cryptology and the imposition of technical measures, the recourse to commissions with experts of different backgrounds, the interference of outsiders due to logistic needs in the field are so many forms of a permanent feature characterising the provisions examined above. Indeed, in order to face the development of computers, which in the first place threatens

the confidentiality of the patient's privacy, these provisions provide for the interference of a growing number of factors from outside the medical world. The Hippocratic Oath, which was only addressed to the physician, turns out to be rather weakened.

It is therefore worth insisting on a self-evident fact. The current evolution must not lead to a destabilisation of the health care relationship. The preoccupations of technical nature and the fears they try to address must not monopolise the attention so much as to overshadow the sometimes-subtle balance essential to a quality relationship between the physician and his or her patient. If they want to take up the computer challenge successfully, the new rules will have to be careful about avoiding two pitfalls.

The first pitfall relates to their content. The risks threatening the respect of private life keep growing ; it is therefore normal that the new generation of provisions tries to guarantee a strengthened protection of private life. The patient's privacy should not be made into an open realm serving the interests of outsiders and community. But neither should it be made into an opaque and inaccessible realm, as wanted by disproportionate rules trying to give the right to private life the status of entitlement right. Making privacy into a sacred and totally inviolable principle equals to destroying the very nature of medical practice. *Any dictatorship of confidentiality should be rejected.* Beyond public health-related considerations, this is required in the interest of the patients themselves.

The second pitfall ensues from an *anarchic and unrealistic development* of the provisions aimed at regulating the health care relationship. Governed by rules from every possible origin, it could turn into defiance. Does that given patient asking to consult his or her electronic medical records meet the conditions set forth by the law ? Has that given physician taken all the suggested or mandatory measures in order to avoid the uncontrolled consultation of the medical data in his or her possession ? The doctor-patient relationship could eventually be less of an alliance against a common enemy — illness — than a struggle between two opponents on the lookout for the slightest mistake of their counterpart. How can such a scenario be avoided if not by stimulating a sense of *professionalism* ? The professionalism of the *physician* who accepts that he or she sometimes has to do without the reassuring refuge of pre-established rules and to find out by him or herself the solution best suited to the patient's needs. The professionalism of the *patient* who dares to trust a professional that he or she cannot fully control for lack of sufficient knowledge.

Acknowledgement

The authors thank Mr. Martin Leloup for expert assistance for translation of the manuscript.

References

1. This first analysis was published as "The protection of the patient's private life : a vast normative landscape" in the previous issue of this journal. It is referred to as "Part One" in the rest of this Article.
2. Also see Michel L. Secret médical et dossier informatisé. *Louvain Méd*, 2001 ; **120** : S125- S132.
3. Van Thuyne D. Intervention at the AMA-UCL Symposium, 24 May 2001.
4. van de Vloed O. (dir.). Fonctions du dossier médical informatisé du médecin généraliste. Website of the EMDMI (Elektronisch Medisch Dossier Médical Informatisé), http://www.health.fgov.be/EMDMI/fr/textes/consensus/fonctdossmed.htm.
5. Heyerick J.P. Données personnelles en matière de santé. Website of the EMDMI, http://www.health.fgov.be/EMDMI/fr/textes/discussion/discuss002.htm.
6. Woodward B. The computer-based patient record and confidentiality. *New Engl J Med*, 1995 ; **333** : 1419.
7. Projet de loi portant des dispositions sociales, Exposé des motifs. *Doc. parl.*, Ch. représ., sess. ord. 1997-1998, n° 1722/1 : 31.
8. Projet de loi portant des dispositions sociales, Exposé des motifs. *Doc. parl.*, Ch. représ., sess. ord. 1997-1998, n° 1722/1 : 31.
9. Woodward B. *Op. cit.* : 1420.
10. Projet de loi portant des dispositions sociales, Exposé des motifs. *Op. cit.* : 31.
11. Woodward B. *Op. cit.* : 1420-1421.
12. *Ibid.* : 1421.
13. *Ibid.* : 1421.
14. *Official Journal of the European Communities*, n° L281 of 23rd November 1995.
15. *Moniteur belge*, 18 March 1993.
16. Similar provisions have been adopted in the legal orders of neighbouring countries. On 6 January 1978, France, for instance, had already adopted Act 78-17 on automatic data processing, files and freedoms. (known as "loi informatique et libertés"). For lack of space, these texts cannot be examined in this Article.
17. Loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. *Moniteur belge*, 3 February 1999.
18. The non-automated processing of personal data is also concerned, provided, though, that these data are contained or likely to appear in a file (art. 3, § 1). The notion of "file" is defined in article 1, § 3. In this way the field of application of the Act is similar to that of Directive 95/46/CE but larger than that of the Convention of the Council of Europe, which only deals with automated data processing.
19. There are exceptions to the rule. The processing need not be carried out under such responsibility when the person whose data are being processed gives written consent to it or when the processing is necessary in order to avoid a concrete danger or to suppress a given penal crime (art. 7, § 4). The supervision of a health care professional seems imperative in all cases set forth in above-mentioned Article 7, § 2, j., insofar as, mentioned in article 7, § 2, j. and not in article 7, § 4, this supervision is part of the definition of the situation in which no interdiction applies.
20. These conditions are set forth in articles 25 to 27 of the Royal Decree of 13 February 2001 implementing the Act of 8 December 1992 on the protection of private life with regards to the processing of personal data. (Arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel) (*Moniteur belge*, 13 March 2001).
21. Loi du 25 janvier 1999 portant des dispositions sociales (*Moniteur belge*, 6 February 1999), article 176.
22. *Moniteur belge*, 30 July 1999.
23. A.R. du 3 mai 1999 portant création d'une Commission «Normes en matière de télématique au service du secteur des soins de santé». *Moniteur belge*, 30 July 1999.
24. *Moniteur belge*, 30 July 1999.
25. See, among others, opinions of 16 April 1994, 22 April 1995, 12 December 1998 and 20 February 1999.

26. See Part One "III. The right to the respect of private life : provisions to differentiated", "The time of elaboration of the provisions".
27. See Part One "III. The right to the respect of private life : provisions to differentiated", "The author of the provisions".
28. These reliability standards are a sign of a today widespread tendency to make cryptology, the traditional science of secrecy, into a real "science of trust" ; guaranteeing confidentiality is no longer enough ; this guarantee has to be recognised as credible.
29. In Belgium, the Act of 8 December 1992 goes so far as to create a new obligation for confidentiality, with possible penal sanctions, rather than referring to an existing obligation. (Projet de loi transposant la directive du 25 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Exposé des motifs. *Doc. parl.*, Ch. représ., sess. ord. 1997-1998, n° 1566/1 : 39).

M. Van Overstraeten
U.C.L. – Faculté de droit
Département de droit public, boîte n° 37
Place Montesquieu 2
1348 Louvain-la-Neuve
E-mail : vanoverstraeten@publ.ucl.ac.be

L. Michel
Surgical Services
Mont-Godinne University Hospital
B-5530 Yvoir, Belgium
E-mail : michel@chir.ucl.ac.be