Security on DNA Database and legislation

1 Introduction

Security of data like those collected by the processing of DNA profiles for subject identification in criminal matters needs to be carefully examined by public institutions.

The stake of security in data processing is a major issue. Security must:
- ensure the availability of services and data,
- prevent the disruption and unauthorised interception of communications,
- confirm that data which has been sent, received or stored are complete and unchanged,
- secure the confidentiality of data,
- protect the information systems against unauthorised accesses,
- protect against attacks involving malicious software,
- secure dependable authentication; (résolConseil012002)

More particularly, in the context which concerns us, it must:
- permit criminal justice to take benefit of technological progress, more particularly, the contribution of genetics for criminal proof,
- offer the citizen warranties of reliability in the establishment of judicial truth which is an essential task for public services.
- Any lack of confidence in this security could possibly slow down the introduction of this "service", a fortiori to extend it.

Both the information system and the organization that ensures its smooth running needs to have the ability to resist to events or actions that could compromise the availability, authenticity, integrity and confidentiality of data.
Many treats are likely to injure the latter:
- Unauthorised access into computer and computer networks would permit the copying or modification of data. This can cause damage both through invasion of the privacy of individuals and through the exploitation of data intercepted.
- Malicious software, such as viruses, can disable computers, delete or modify data. This can be extremely destructive and costly.
- Misrepresentation of people or entities can cause substantial damages. For example, one may be considered as a trusted source, and confidential information may thus be sent to the wrong persons.
- Many security incidents are due to unforeseen and unintentional events such as natural disasters (floods, storms, earthquakes), hardware or software failures, and human error. (Com2001/298)

These risks must be considered as significantly important since the nature of these data (health related personal data) and the use they are intended to (the establishment of judiciary truth) is very sensitive.

Various technical or organisational measures can be taken to prevent or give the possibility to react against internal or external treats.

Nevertheless, one must keep in mind that the stakes of security, the encountered risks and the necessity of taking measures are perceived differently according to :

- the person concerned by these data (this person wants to protect his privacy)
- the person who processes the data (the user) (who looks for a better functionality to perform his mission which is to manage a DNA database)
- the third party authorized to receive the data (who wants to keep the possibility to use the data with an easy access)

and finally

- the non-authorized third party (for whom motivations can be quite different)

The sensitivity of these four actors may vary regarding their own interest and the constraints that such security measures imply to them. Implementation of these measures must be done proportionally to the encountered risks and the costs it implies.

It is this difficult combination of interests (privacy, functionality, accessibility, secret of the investigation) and the delicate proportionality between the encountered risks and the means of security (cost) that law tends to adjust.

Law isn't the exclusive way to ensure security of databases.
The European commission, in its communication (2001) 298, only perceives the legislative way as a means among others to construct its politic of network and information security.

Law has nevertheless direct impacts on any of these four "actors", trough different legislations (privacy, DNA, electronic signature, cyber crime, phone-tapping,…). We are here in a European context, but we can not leave aside national rules. Examining the Belgian example, we can perceive the different legislative flows that are considering the question of data security. From now on we can evoke the orientation of the European politic in this matter.

2 Belgian legislation

The aspects of data security in the processing of DNA profiles for identification purposes in criminal matters are not only pursued by the DNA law[1]. Other legal rules can ensure a securised management of such data. These are principally : the privacy law[2], the law on electronic signature[3], and the law on cybercrime[4].

We are here reviewing the point of view of the person concerned by these data, of the internal user, of the authorized third party and the unauthorized third party. This, in order to underline the rules that apply to each of them in terms of security.

[1] See Law of 22 March 1999 on the procedure for identification using DNA profiling in the criminal justice system, published in the official journal of Belgium 20 May 1999, err. 24 June 1999. To put this law and its practical modalities into force, a royal decree is still needed. For the parliamentary procedures, see Chamber Documents, 1996-1997, nr. 1047/1-8.

[2] Law of 8 December 1992 on the protection of privacy in regard to the electronic processing of personal identity data, adjusted (amended) by the law of 11 December 1998 concerning the implementation of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals in regard to the processing of personal data and on the free movement of such data.

[3] Law of 9 July 2001 in which certain regulations are laid down (determined) concerning the legal framework for electronic signatures en certification services, published in the official journal of Belgium, 29 September 2001, pg. 33070.

[4] Law of 28 November 2000 on computer crime, published in the Official Journal of Belgium, 3 February 2001, pg. 2909.

2.1 The concerned person

From the person concerned's point of view, security consists in following points :
- Only authorised data should be processed;
- If the processing is authorized, data must be up-to-date and complete;
- Data should only be processed for legitimate purposes and used in a way compatible with these purposes;
- Data is only processed by authorized persons.

2.1.1 Privacy law

The privacy law settles questions of purpose, accuracy, access etc…
Without detailing these provisions, one can underline that the text that protects the person, usually provides a correspondent obligation for the controller.
Thus, for example, regarding the question of accuracy of data, Article 4 § 1er holds that Personal data shall be: (…) 4° accurate and, if necessary, kept up to date, This implies for the controller that :

> every reasonable step shall be taken to ensure that data that are inaccurate or incomplete, having regard to the purposes for which they are collected or for which they are further processed, are erased or rectified;.

2.1.2 DNA law

When reading the DNA law one asks the question of what security measures are to be adopted, the conclusions are the following :
-Many global warranties are taken on the drawing of the sample and its destruction, the analysis, the recording and the keeping of profiles in the database, the access to these data, ….
These are all measures that contribute to security.

<u>Recording and keeping</u>
- The recording is done in accordance with the law (art. 5, § 1, al. 4 DNA law) or by order of the magistrate (art. 44ter, §2, al.3 C.I.Cr. et art. 5, § 2, al. 1 DNA law) ;
- One can only record data according to? ..determined ?by law (44ter, § 1er, al. 2 et § 2, al. 4 C.I.Cr., art. 4, § 1er, al. 2, art. 4, § 3, al. 4 et art. 5, § 4, al. 4 DNA law)
- And only for a duration determined by law (art. 4, § 4 et art. 5, § 5 DNA law)

<u>The use of data is permitted</u>
- Only in order to establish an identification link (art. 44ter, § 1er, al. 1 C.I.Cr., art. 4, § 2 et art. 5, § 3 loi ADN)- it is this law that determines the purpose of DNA databases.
- Only by authorized persons (art. 44ter, § 2, al. 3 C.I.Cr, art. 4, § 3, al. 1 loi ADN)

<u>Regarding the access</u>
- Only the public prosecuter or the examining judge can know the identity of the person related to the relevant DNA profiles of the database. (art. 4, § 3, al. 2 et art. 5,§ 4, al. 2 loi ADN)

But one can regret that regarding the specific question of confidentiality and protection warranties, the law only holds the designation of an officer for the protection of personal data at the INCC (article 7, al. 2, 2° et al. 3 loi ADN), and the adoption of a future decree that will detail the modalities of the processing (according to article 7, al. 2, 1° loi ADN);

In accordance with this law, criminal sanctions are possible if there is:
- A voluntary reading by a non authorized person of the results of the analysis (art. 6, § 1 loi ADN);
- A use for other purposes than to establish an identification link (art. 6, § 2 loi ADN)

2.2 The user

The security for the user applies not only to the internal risks but also to the external breaches. Various laws examine this question. More particularly, the privacy law distinguishes different persons. It lays down many different obligations for the controller but also for the user acting under his authority.

2.2.1 Privacy law

According to the privacy law

The controller
§ 2. The controller shall, among other:

1° watch carefully that the data are updated, that inaccurate, incomplete and irrelevant data, as well as data that have been obtained or further processed in violation of the privacy law, are corrected or erased;

2° take care that the access to the data and possibilities of processing by the persons who are acting under his authority, are limited to what is necessary for the fulfilment of their duties or for the requirements of the service;

3° notify all persons acting under his authority about the provisions of this law, as well as about all relevant provisions in respect of the protection of the privacy with regard to the processing of personal data;

§ 4. In order to guarantee the security of personal data the controller shall take the appropriate technical and organisational measures that are necessary for the protection of personal data against all the treats we saw before (accidental or unauthorised destruction, accidental loss, as well as against alteration of, access to and any other unauthorised processing of personal data).

These measures shall ensure an appropriate level of security taking into account the state of the art in this field and the cost of implementing the measures on the one hand, and the nature of the data to be protected and the potential risks on the other hand.

The law holds specific obligations regarding security for the controller if the processing is consigned to a processor

The person acting under the authority of the controller (or of the processor, as well as the processor himself having access to the personal data,) may only process the personal data on the instructions of the controller, except for the case of an obligation imposed by or by virtue of a law, decree or ordinance..

Finally, none of the numerous sanctions of the privacy law punishes the non-respect of these obligations.
On the contrary, in the event of damage caused by the non-respect of these obligations, a civil liability action could be undertaken**.**

2.2.2 DNA law

Except the sanctions that punish some abuses (voir supra), there is nothing specifically mentioned in terms of positive obligations for the INCC in which DNA databases are created to guarantee the security neither for the controller nor for the persons acting under his authority.
Law only specifies the role of the data protection officer.
Only the decree to come will have to consider the recording modalities, the processing and the use of DNA profiles in DNA databases.

2.2.3 Cybercrime law

The cybercrime law lays down sanctions for any authorized person who bypasses his access power.

2.3 Communication to third parties

2.3.1 DNA law

DNA law only envisages one case of communication of data from the DNA data base: When the comparison expertise establishes a positive link with other DNA profiles of the database, the expert automatically informs the competent magistrates (art . 5, § 4, al. 5 et art. 4, § 3, al. 3 loi ADN) ;

Apart from this, there are or precisions of the law (especially in the absence of a decree) for example concerning the relations between the INCC and the other analysis laboratories in Belgium or abroad….

Nothing is specified concerning the transborder transfer of personal data. One needs to refer to the general rules, which constitute privacy law, and to the rules of judicial cooperation.

In accordance with the rules of judicial cooperation, the communication queries needs to follow the rules of the Convention of 59, in fact by the rogatory Commission or by request for mutual assistance.

2.3.2 Privacy law

If communication is necessary and intended to a processing with a compatible purpose, the privacy law does not lay down any obstacles to the transmission of data in a country of the European community, since they are all subject to the same requirements provided by the European directive 95/46 on data protection.

For transmission of data to a country outside the European community, the third country must ensure an adequate level of protection. The adequacy of the level of protection shall be assessed in the light of, among other, security measures that are complied with in that country.

Moreover**,** as a derogation from this requirement, a transfer of personal data to a country outside the European Community may take place if the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims;

2.3.3 Law of 9 July 9 2001 on electronic signature

This law settles the use of cryptography techniques and is thus important regarding the question of security of data in DNA databases. This technique that will be presented by my friend and previous colleague Jean-Marc DINANT, consists in encoding data with a double purpose.
On one hand this aims at ensuring confidentiality in the transmission of data. On the other hand, this permits certain identification of the sender of the data and of the addressee. A same technique can thus encounter these two important purposes in security matters.

2.4 Non-authorized third parties

The first objective of the law is the dissuasion by penalisation of some particular acts. If these acts are committed this could be punished.

2.4.1 Law on cybercrime

Law on cybercrime lays down many sanctions. It punishes in particular computer forgery. It is the fact of getting into an informatics system, modifying or deleting data. It is also the fact of modifying by any technological means the possible use of the data in an informatics system, and thus modifying the legal impact of these data.
It is finally also the fact of intentional use of incorrect data.

The law defines as offences attempts at confidentiality, integrity, and availability of computer systems and data that are kept or transmitted trough these systems, like access or intentional maintenance by a non-authorized person into a computer system. In this case, law punishes the fact

of taking data, to use them or to cause a damage, even non intentional, to the computer system or the data.

2.4.2 Phone tapping law

If the intrusion of a non-authorized third party uses the phone network, law prohibits any tapping, reading and recording of communications or private telecommunications. It punishes the following acts:

- tapping, reading and recording
- Installation of any device in order to tap, read or record;
- To possess, reveal, disclose the contents of illegally tapped or recorded telecommunications.

2.4.3 DNA law

Sanctions are possible if there is

- A voluntary reading of the results of the analysis by a non-authorized person (art. 6, § 1 loi ADN);
- Voluntary use of the illegally obtained data for other purposes utilisation (art. 6, § 2, 1° loi ADN);

2.4.4 Privacy law

The privacy law lays down sanctions too.

3 Conclusion

This overview of Belgian legislation, in the same way as the analysis of European legislation, enables to highlight three legal trends in the context of the security of data :

A first trend is constituted of rules in telecommunication matters and data protection.
It aims to frame the action of telecommunication operators and to warrant a respectful processing of data and of the privacy of the concerned person.

A second trend contains the rules in cybercrime. This is meant essentially to dissuade and punish if applicable, the attitude of a non-authorised third party.

A third trend, which is developing, focuses especially on network security. Legislations related to electronic signature fall into this trend. Other legislations will progressively be added either to reinforce the legal arrangements of the first two trends or in creating specific rules.

One can notice that on a European level, security measures of data in any new instrument will be established. Especially for those related in the sector of Justice and Home affairs (JAI). It is for example the case of the Europol Convention, or in the Eurodac rule (comparison of fingerprints of the applicants for asylum)

To conclude, one must stress that proportionality must, on the one hand guide the choices of security measures in view of the risks, and on the other hand between the interests of protection which conflict with the practical side of the adoption of the measures. The right to privacy is a fundamental right laid down in the European Convention on Human rights and in the European charter of fundamental rights. In this respect it must always be preferred when the balance of interests does not enable to determine the attitude to adopt in terms of security of data.

Bertrand RENARD bertrand.renard@just.fgov.be
Research Assistant
Departement of Criminology
NICC
Ministry of Justice
Belgium