Cryptography in Belgian Law

Antoine, Mireille

Published in:
The EDI Law Review

Publication date:
1996

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

The EDI Law Review 3: 221–228, 1996.

Cryptography in Belgian Law

MIREILLE ANTOINE
Centre de Recherches Informatique et Droit, Namur-Cellule Interfacultaire de Technology Assessment, Namur

1. Introduction

Together with the advances in telecommunications development, a necessity has emerged to effectively increase the security of the information transmitted. This tends towards two goals: either enabling the authentication of messages or ensuring their confidentiality.

The authentication of documents allows one to be certain that a document has genuinely been sent by an authorized person (source authentication) and that it has not been illegally tampered with en route (content authentication). Data confidentiality assures that the significance of information is not grasped other than by authorized persons (any unauthorized persons being denied access to the information transmitted).[1]

One effective way to ensure the security of information transmitted through a network involves cryptography: an "electronic bug" incorporated in the transmission terminal transforms the "clear" text into a coded message which is in turn deciphered and reconstituted into its original form thanks to a similar device integrated into the recipient's receiving terminal.[2]

Although this security technique offers various advantages, it may nonetheless pose problems for tapping operations carried out within the framework of the 1994 Belgian privacy law (30th of June) relating to freedom from tapping, unauthorized appraisal or recording of private telecommunications.

We must examine this law more closely to better understand the legal problems posed by cryptography in Belgium (1). Our reading should be complemented by a reading of Articles 202 and 203 of the law of the 21st of December 1994 ("portant des dispositions sociales et diverses") amending the law of the 21st of March 1991 bearing on the reform of certain state enterprises (2).

2. The Privacy Law of the 30th of June 1994 Relative to Freedom from Tapping, Unauthorized Apprehension of Information or Recording of Private Telecommunications

The aim of this law is to enshrine the principle of the protection of privacy from audio surveillance while, nonetheless, authorizing the same when justified by the necessities of the fight against terrorism and organized crime.

The law's field of application is clearly defined. It applies as much to *communications* as to *telecommunications*, these latter consisting of "any transmission, broadcast or reception of signs, signals, writings, images, sounds or data of any nature, via wire, radio, optical signals or any other electromagnetic systems" (Article 68,4° of the above mentioned law of the 21st of March 1991). Furthermore these communications and telecommunications must be "*private*." Considered as such are any not intended to be heard by everyone.

The ability to carry out taps must be considered as an exception to the general principle that such interventions are forbidden. The cases in which such a practice is justified and the procedure to be applied are both strictly defined by law.[3]

It should be noted that such tapping, appraisal or recording of communications or telecommunications must take place *during* transmission, and that any communications or telecommunications that are the object of surveillance measures must be *recorded, transcribed* and, if necessary, *translated*.

In order to prevent the law on tapping from becoming devoid of sense, it is indispensable that, in parallel, the degree of telecommunications regulation be adapted. This is the object of the law of the 21st of December 1994.

3. The 21st December 1994 Law Bearing on Social and Various Other Provisions

The law of the 21st December 1994 bearing on social and various other provisions comes as an amendment to the 1991 law (21st of March) on state enterprise reform, inserting two new provisions, the first relating to the technical means at the disposal of network operators when allowing application of the tapping law (Article 70 bis), the second to the type of terminals licenced for use (Article 95, clause 1).

Article 70 Bis

The 1991 law (21st of March) on reform of certain state owned companies gives weight to the principle (Title III, Chapter II, "Dispositions générales") that all kinds of telecommunications activities, other than public ones, are

inherently free of control and that this principle may only be derogated if public safety or the defense of the realm demand it (Article 70). It is in this context that the new Article 70 bis has been inserted, investing the King with the task of fixing by decree, after deliberation in the Council of Ministers, the means by which Belgacom, the national telecom operator, and purveyors of designated non-reserved services are to permit, depending on the needs of the case, the tapping law of 30th June 1994 to be applied.

This adaptation is included in the annex of Article 90 quater, §2 of the code of criminal procedure (introduced by the law on tapping), which envisages the possibility for the examining magistrate of calling for a *technical tender to be held for network operators* prior to a tapping surveillance operation.

Operators are therefore obliged to make sure that surveillance and tapping are technically possible on their infrastructures, equipment and services. In any case the following is required:

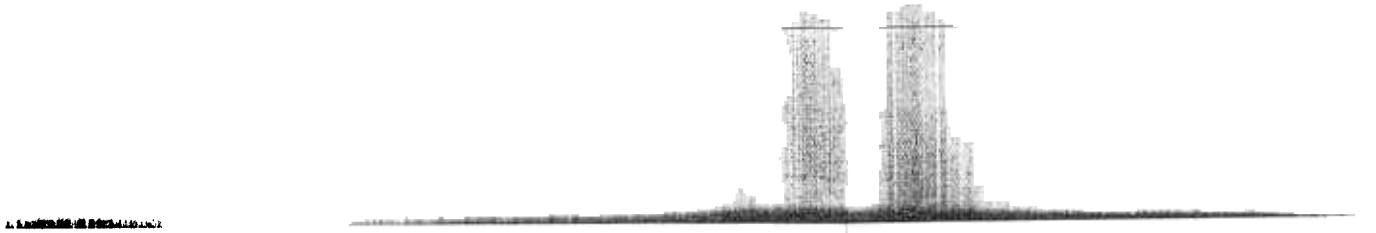
- Determination of the technical means that necessarily must be set up if such a goal is to be realized. No royal decree has been adopted as yet.
- Remaining within financial limits acceptable to network operators. Indeed, under the obligation to ensure that communications can be tapped, depending on their province, the financial cost falls to the operators. This is naturally not the case when their assistance is solicited within the framework of the tapping law.[4] The question of tarification has yet to be resolved in this case.

3.2. *Article 95, 1st Clause*

The first clause of Article 95, figuring in Chapter VIII, "Terminal equipment" envisages a new possibility for the Minister, based on a suggestion from the Belgian Institute of Post and Telecommunications, to withdraw licensing or prohibit connection to a public telecommunications infrastructure to any terminal equipment of which it has been demonstrated that the equipment in question renders the technical means to apply the 30 June 1994 tapping law ineffective. The hypothesis here envisioned is, of course, that of equipment enabling the encryption of transmissions into code.

Article 95, 1° to 4° enumerates a series of situations in which the licence for a terminal could be revoked, such as when: the equipment no longer corresponds technically to that which was licenced (1°), the use for which it was approved no longer corresponds to its current use (3°), it no longer conforms to the currently required technical norms (2°) or is the source of damage to the infrastructure in question or of danger to Belgacom personnel (4°).

Was it strictly necessary to add to this list the hypothesis under which the terminal equipment in question hinders the application of the tapping law



(5°)? We rather think not, inasmuch as the technical specifications underlying the licencing of a telecommunications terminal are determined by ministerial decree (Article 94, §2). It would have been sufficient, at the level of this ministerial decree, merely to delineate the technical norms deemed necessary in order to render the application of the phone tapping law effective. Within such a hypothesis, the revoking of a licence could take place on the basis of 2°. By introducing measure 5°, the legislator has established an arbitrary provision, since no such technical norm justifying the loss of a licence has yet been fixed.

It is sufficient to remind ourselves on this account that the Convention to safeguard human rights and fundamental liberties lays down, in Article 8 §1, the principle under which "every person has the right to the respect of privacy: in their private and family life, their home and correspondence," a principle to which exceptions can only be permitted under the conditions set out in §2.[5]

If we refer to the jurisprudence of the European Court of Human Right it is clear that the law "must define the extent and the rules of procedure for such a power with sufficient clarity – taking into account the legitimacy of the aim pursued – to provide the individual with adequate protection against arbitrary treatment."[6]

4. Lines of Reflection on Which to Base Amendments to Articles 70 Bis and 95

Although the aim envisaged by Articles 70 bis and 95 is to guarantee effective application of the acoustic surveillance or tapping law[7] and not to prohibit or restrict the commercialization and use of apparatus designed to ensure the confidentiality of communications,[8] there is no doubt that enforcement of the current legislation is not only going to come up against the jurisprudence of the European Court of Human Rights, but also hangs a question mark over the latest developments in information security technology.

Effective cryptography regulation, that respects democratic values, cannot be conceived without taking the following aspects into consideration.

4. *Initiatives at the Level of International Organizations*

Work is currently being carried out by organizations at the international level, whether within the O.E.C.D., the I.C.C. or the E.U., primarily bearing on the different recommendations adopted at the European level, as well as the Green Paper and the proposal for a Green Paper respectively relative to the protection of encrypted services in the internal Market and the security of information systems.

4.2. *Harmonization of Cryptography Regulations*

The Green Book on cryptographic services protection underlines the necessity of a Community level initiative to ensure the judicial protection of such services against illicit radio reception by specifically excluding from the covert services, "encrypted services designed to ensure the integrity and confidentiality of transmitted messages, viz financial and telecommunications services. . . ."[9]

At this time when we are witnessing the convergence of telecommunications and audiovisual technology, regulatory harmonization for cryptography becomes crucial. We cannot run the risk of adopting contradictory regulations for radiophonic diffusion and telecommunications.[10] One step has certainly been taken recently by the European Commission, which, aware of the necessity of harmonizing regulations relative to both sectors, has announced the intention of having a study carried out into those questions raised by "the adaptation of the E.U. regulatory framework in the field of telecommunications to the expanding multimedia environment." The adoption of cryptography regulations common to both sectors must be a priority. We must note, however, that the adaptation of such measures to Belgian legislation cannot be made painlessly, due to the clash between the different competent authorities.

4.3. *Harmonization of the Various National Legislations*

The necessity of harmonizing regulations relative to cryptography is equally felt at the national level in the legislations of the different member States of the E.U. due to the international dimension of communications (and the transborder data flow thus engendered), radio transmissions and multi-media services. Disparities between national legislations will inevitably lead to the emergence of "a paradise for computer criminals."[11]

4.4. *Cryptography as a Legal Method for the Safeguarding of Data*

Article 17 of the European Directive on the protection of individual persons with regard to the processing of their personal data and the free flow of data imposes that an appropriate level of security must surround the processing of data (notably when such processing involves the transmission of data into or within a network). Four parameters condition the choice of security measures employed: the state of the art, the cost, the risks presented by the process itself and the nature of the data to be protected. These same parameters are to be found listed under Article 16, §3, clause 2 of the Belgian law of the 8th of December 1992 relating to the protection of privacy with regard to the processing of data of a personal nature.

Furthermore, the law accords the King the right, on the advice of the Commission for the protection of privacy, to decree those norms deemed appropriate in that which concerns a cyber security for all or certain categories of data processing (clause 3). Cryptography might become the required security measure for the processing of certain data within the above cited parameters . . . and thereby imposed on third party countries (Article 25 of the Directive).

4.5. *Criteria for Adopting Technical Measures Rendering Tapping Surveillance Possible*

Finally the vital question must be asked to which, it seems, no state has as yet provided a satisfactory answer, a question of paramount importance to the development of information superhighways: how do we reconcile citizen's rights with state prerogatives?[12]

Three determinant criteria must guide the choice of a solution that permits the surveillance of encrypted communications within the framework of a tapping procedure:

- *security*: no measure permitting tapping may lead to a weakening of security. Control of security measures must consequently rest in the hands of those who adopted them;
- *cost*: the solution adopted may not involve a disproportionate charge to those individuals or legal entities who use cryptography for their data security;
- *flexibility*: it is as true of telecommunications security as it is of that designed to guarantee the protection of personal data: there is no method capable of ensuring complete information security. Data security measures must grant an adequate level of protection according to the nature of the communications one wishes to protect (see point 4.4). Consequently, no solution should seek to impose a single standard of security on all communications.

4.6. *A Short Commentary on Recently Proposed Amendments*

Two draft bills have recently been laid before the Belgian Senate,[13] both of which suggest the abrogation of the two provisions commented above.

The second has the merit of offering an alternative. While recognizing that to prohibit the use of cryptography would be disproportionate to the aim of ensuring necessary tapping access, it recognizes also the need to find a solution to the tapping question, setting aside directly the "key escrow" technique. With regard to the criteria enumerated above, this solution is difficult to defend because, on the one hand, it weakens security because it involves a "plundering of keys," and, on the other hand, it demands a level of investment disproportionate to the aim pursued.

The idea suggested in the draft bill is the following: within the course of legal proceedings, the examining magistrate may "call upon assistance in the decryption of a message from any person considered capable of giving such assistance, if serious grounds exist to consider the matter in which the message has been taken in evidence as constituting an infraction as envisaged under the law (. . .) and if other means of investigation are deemed insufficient to a full exposure of the truth" (Article 91 bis).

In order to make the examining magistrate's task easier and to avoid any mishap, it would be advisable to designate a "person responsible"[14] for cryptography, one of whose functions would be that of privileged interlocutor in the event of a tapping operation. This solution presents two guarantees: the first is that security would not be shared with a third party (as is the case with the "key escrow" system), and the second is that the examining magistrate would immediately know who to turn to.

Without entering into details, this technique nonetheless presents some imperfections which call for improvement.

5. Conclusion

Thanks to the privacy law relating to freedom from tapping, unauthorized apprehension of information or recording of private telecommunications, citizen's privacy has been granted effective legal protection. However, the law authorizes, as an exception in a restricted number of cases, tapping operations, so long as these are necessary to effectively combat terrorism and organized crime.

Nonetheless, the use of certain techniques, such as cryptography, may render such tapping operations difficult, if not impossible. Recently the idea has surfaced in Belgium, as in many other countries, to regulate the use of cryptography. Urgency is often a poor counsellor, as an evaluation of Belgian legislation on the subject has amply demonstrated. However, the political world is apparently aware of this, if the two draft bills recently introduced before the Belgian Senate can be taken as an indicator.

Whatever happens, a democratic solution that reconciles the various interests involved cannot be conceived without taking into account the guidelines which emerge from the various studies carried out by the international organizations (O.E.C.D., I.C.C., E.U.) on the one hand, and, on the other, the three parameters of cost, security and flexibility.

The objective consists in finding the precarious equilibrium between the respect of privacy and the necessity of combatting serious organized crime.

Notes

1. J. Hubin,, "La Sécurité informatique," *Cahier de C.R.I.D.*, n° 11, Bruxelles, Kluwer, 1996, to be published.
2. H. Maisl, "Communications mobiles, secret des correspondances et protection des données personnelles," *D.I.T.*, 1995/2, p. 14.
3. For a more in depth study of the question, see H.-D. Bosly, D. Vandermeersch, "La loi belge du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise connaissance et l'enregistrement de communications et télécommunications privées," *Rev. dr. pen. et crim.*, 1995, pp. 301–343; T. Henrion, "Les écoutes téléphoniques," *J.T.*, pp. 205–213.
4. Exposé des motifs, *Doc. parl.*, Sénat, 1994–1995, 1218-1, 88.
5. These principles were reaffirmed by the Council of Europe in the Recommendation R(95)4 on the protection of data of a personal nature in the field of telecommunication services, with reference particularly to telephone services. It suggests that network operators and purveyors of services, equipment and software participate in "information technology to manufacture and exploit networks, equipment and software that respect the privacy of users" and offers them anonymous modes of telecommunication network and system access.
6. E.C.H.R., case Malone, judgment of 2 August 1984, A Series, n° 68.
7. Note in this context the conformity of Belgian legislation to Recommendation R(95)13 of the Council of Europe relative to problems of penal procedure connected to information technology.
8. Rapport de la commission de l'infrastructure au Sénat, *Doc. parl.*, Sénat, 1994–1995, 1218-9, 3.
9. Tender for offers concerning a study on the adaptation of the regulatory framework of the E.U. in the field of telecommunication to the expanding multimedia environment, O.J. of 12.6.1996, N° C 168/18.
10. For a deeper study of the European legislation for the telecommunications and audiovisual sector, see for example S. Bazzanella, R. Queck, V. Willems, "Le régime juridique de la fourniture de services multimédias en Belgique," *Auteurs et Media*, juin 1996, n° 2.
11. Y. Poullet, V. Willems, C. Lobet-Maris, *Vers une société de l'information*, Cahier du C.R.I.D., n° 10, Bruxelles, Story Scientia, 1995, p. 53.
12. H. Maisl, "Communications mobiles, secret des correspondances et protection des données personnelles," *D.I.T.*, 1995 n° 2, p. 19.
13. Proposition de loi abrogeant les articles 70 bis et 95, alinéa 1°, 5°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, *Doc. parl.*, Sénat, 1995–1996, 1-343/1; Proposition de loi abrogeant les articles 70 bis et 95 de la loi du 21 décembre 1991 portant réforme de certaines entreprises publiques économiques et complétant le Code d'instruction criminelle afin de donner un cadre à l'aide au décryptage des messages, *Doc. parl.*, Sénat, 1995–1996, 1-352/1.
14. The designation of a responsible person, for emergencies, for reproduction or recording, was one of the ideas which underlay the Recommendation R(81) 20 of the Council of Europe relative to aligning legislations in the field of the demands of the law and in the matter of the admissibility in evidence of electronic documents and computer recordings.