Possible relevant data protection and privacy cases CJEU + ECtHR

Nr	ECtHR Judgement/Opinion	Paragraph/Text
1	Eur. Court HR, *Klass and others v. Germany* judgment of 6 September 1978, 5029/71: interception of correspondence and telephone communications; secret surveillance; interests of national security; prevention of disorder or crime; adequate and effective guarantees against abuse; judicial control	41. The first matter to be decided is whether and, if so, in what respect the contested legislation, in permitting the above-mentioned measures of surveillance, constitutes an interference with the exercise of the right guaranteed to the applicants under Article 8 para. 1 (art. 8-1). **Although telephone conversations are not expressly mentioned in paragraph 1 of Article 8 (art. 8-1), the Court considers, as did the Commission, that such conversations are covered by the notions of "private life" and "correspondence" referred to by this provision.** In its report, the Commission expressed the opinion that the secret surveillance provided for under the German legislation amounted to an interference with the exercise of the right set forth in Article 8 para. 1 (art. 8-1). Neither before the Commission nor before the Court did the Government contest this issue. Clearly, any of the permitted surveillance measures, once applied to a given individual, would result in an interference by a public authority with the exercise of that individual's right to respect for his private and family life and his correspondence. Furthermore, in the mere existence of the legislation itself there is involved, for all those to whom the legislation could be applied, a menace of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunication services and thereby constitutes an "interference by a public authority" with the exercise of the applicants' right to respect for private and family life and for correspondence. The Court does not exclude that the contested legislation, and therefore the measures permitted thereunder, could also involve an interference with the exercise of a person's right to respect for his home. However, the Court does not deem it necessary in the present proceedings to decide this point. 42. **The cardinal issue arising under Article 8 (art. 8) in the present case is whether the interference so found is justified by the terms of paragraph 2 of the Article (art. 8-2). This paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be narrowly interpreted. Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions.** 43. In order for the "interference" established above not to infringe Article 8 (art. 8), it must, according to paragraph 2 (art. 8-2), first of all have been "in accordance with the law". This requirement is fulfilled in the present case since the "interference" results from Acts passed by Parliament, including one Act which was modified by the Federal Constitutional Court, in the exercise of its jurisdiction, by its judgment of 15 December 1970 (see paragraph 11 above). In addition, the Court observes that, as both the Government and the Commission pointed out, any individual measure of surveillance has to comply with the strict conditions and procedures laid down in the legislation itself.

44. It remains to be determined whether the other requisites laid down in paragraph 2 of Article 8 (art. 8-2) were also satisfied. According to the Government and the Commission, the interference permitted by the contested legislation was "necessary in a democratic society in the interests of national security" and/or "for the prevention of disorder or crime". Before the Court the Government submitted that the interference was additionally justified "in the interests of ... public safety" and "for the protection of the rights and freedoms of others".

45. The G 10 defines precisely, and thereby limits, the purposes for which the restrictive measures may be imposed. It provides that, in order to protect against "imminent dangers" threatening "the free democratic constitutional order", "the existence or security of the Federation or of a Land", "the security of the (allied) armed forces" stationed on the territory of the Republic or the security of "the troops of one of the Three Powers stationed in the Land of Berlin", the responsible authorities may authorize the restrictions referred to above (see paragraph 17).

46. The Court, sharing the view of the Government and the Commission, finds that the aim of the G 10 is indeed to safeguard national security and/or to prevent disorder or crime in pursuance of Article 8 para. 2 (art. 8-2). In these circumstances, the Court does not deem it necessary to decide whether the further purposes cited by the Government are also relevant. On the other hand, it has to be ascertained whether the means provided under the impugned legislation for the achievement of the above-mentioned aim remain in all respects within the bounds of what is necessary in a democratic society.

48. **As the Delegates observed, the Court, in its appreciation of the scope of the protection offered by Article 8 (art. 8), cannot but take judicial notice of two important facts. The first consists of the technical advances made in the means of espionage and, correspondingly, of surveillance; the second is the development of terrorism in Europe in recent years. Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime.**

49. **As concerns the fixing of the conditions under which the system of surveillance is to be operated, the Court points out that the domestic legislature enjoys a certain discretion. It is certainly not for the Court to substitute for the assessment of the national authorities any other assessment of what might be the best policy in this field (cf., mutatis mutandis, the De Wilde, Ooms and Versyp judgment of 18 June 1971, Series A no. 12, pp. 45-46, para. 93, and the Golder judgment of 21 February 1975, Series A no. 18, pp. 21-22, para. 45; cf., for Article 10 para. 2, the Engel and others judgment of 8 June 1976, Series A no. 22, pp. 41-42, para. 100, and the Handyside judgment of 7 December 1976, Series A no. 24, p. 22, para. 48). Nevertheless, the Court stresses that this does not mean that the**
Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even

destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.

50. **The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law.** The functioning of the system of secret surveillance established by the contested legislation, as modified by the Federal Constitutional Court's judgment of 15 December 1970, must therefore be examined in the light of the Convention.

51. According to the G 10, a series of limitative conditions have to be satisfied before a surveillance measure can be imposed. Thus, the permissible restrictive measures are confined to cases in which there are factual indications for suspecting a person of planning, committing or having committed certain serious criminal acts; measures may only be ordered if the establishment of the facts by another method is without prospects of success or considerably more difficult; even then, the surveillance may cover only the specific suspect or his presumed "contactpersons" (see paragraph 17 above). Consequently, so-called exploratory or general surveillance is not permitted by the contested legislation. Surveillance may be ordered only on written application giving reasons, and such an application may be made only by the head, or his substitute, of certain services; the decision thereon must be taken by a Federal Minister empowered for the purpose by the Chancellor or, where appropriate, by the supreme Land authority (see paragraph 18 above). Accordingly, under the law there exists an administrative procedure designed to ensure that measures are not ordered haphazardly, irregularly or without due and proper consideration. In addition, although not required by the Act, the competent Minister in practice and except in urgent cases seeks the prior consent of the G 10 Commission (see paragraph 21 above).

52. The G 10 also lays down strict conditions with regard to the implementation of the surveillance measures and to the processing of the information thereby obtained. The measures in question remain in force for a maximum of three months and may be renewed only on fresh application; the measures must immediately be discontinued once the required conditions have ceased to exist or the measures themselves are no longer necessary; knowledge and documents thereby obtained may not be used for other ends, and documents must be destroyed as soon as they are no longer needed to achieve the required purpose (see paragraphs 18 and 20 above). As regards the implementation of the measures, an initial control is carried out by an official qualified for judicial office. This official examines the information obtained before transmitting to the competent services such information as may be used in accordance with the Act and is relevant to the purpose of the measure; he destroys any other intelligence that may have been gathered (see paragraph 20 above). 53. Under the G 10, while recourse to the courts in respect of the ordering and implementation of measures of surveillance is excluded, subsequent control or review is provided instead, in accordance with Article 10 para. 2 of the Basic Law, by two bodies appointed by the people's elected representatives, namely, the Parliamentary Board and the G 10 Commission. The competent Minister must, at least once every six months,

report on the application of the G 10 to the Parliamentary Board consisting of five
Members of Parliament; the Members of Parliament are appointed by the Bundestag in proportion to the parliamentary groupings, the opposition being represented on the Board. In addition, the Minister is bound every month to provide the G 10 Commission with an account of the measures he has ordered. In practice, he seeks the prior consent of this Commission. The latter decides, ex officio or on application by a person believing himself to be under surveillance, on both the legality of and the necessity for the measures in question; if it declares any measures to be illegal or unnecessary, the Minister must terminate them immediately. The Commission members are appointed for the current term of the Bundestag by the Parliamentary Board after consultation with the Government; they are completely independent in the exercise of their functions and cannot be subject to instructions (see paragraph 21 above).

54. The Government maintains that Article 8 para. 2 (art. 8-2) does not require judicial control of secret surveillance and that the system of review established under the G 10 does effectively protect the rights of the individual. The applicants, on the other hand, qualify this system as a "form of political control", inadequate in comparison with the principle of judicial control which ought to prevail. It therefore has to be determined whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" resulting from the contested legislation to what is "necessary in a democratic society".

55. **Review of surveillance may intervene at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding the individual's rights. In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 para. 2 (art. 8-2), are not to be exceeded. One of the fundamental principles of a democratic society is the rule of law, which is expressly referred to in the Preamble to the Convention (see the Golder judgment of 21 February 1975, Series A no. 18, pp. 16-17, para. 34). The rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure.**

56. Within the system of surveillance established by the G 10, judicial control was excluded, being replaced by an initial control effected by an official qualified for judicial office and by the control provided by the Parliamentary Board and the G 10 Commission. **The Court considers that, in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge.** Nevertheless, having regard to the nature of the supervisory and other safeguards provided for by the G 10, the Court concludes that the

exclusion of judicial control does not exceed the limits of what may be deemed necessary in a democratic society. The Parliamentary Board and the G 10 Commission are independent of the authorities carrying out the surveillance, and are vested with sufficient powers and competence to exercise an effective and continuous control. Furthermore, the democratic character is reflected in the balanced membership of the Parliamentary Board. The opposition is represented on this body and is therefore able to participate in the control of the measures ordered by the competent Minister who is responsible to the Bundestag. The two supervisory bodies may, in the circumstances of the case, be regarded as enjoying sufficient independence to give an objective ruling.
The Court notes in addition that an individual believing himself to be under surveillance has the opportunity of complaining to the G 10 Commission and of having recourse to the Constitutional Court (see paragraph 23 above). However, as the Government conceded, these are remedies which can come into play only in exceptional circumstances.

57. **As regards review a posteriori, it is necessary to determine whether judicial control, in particular with the individual's participation, should continue to be excluded even after surveillance has ceased. Inextricably linked to this issue is the question of subsequent notification, since there is in principle little scope for recourse to the courts by the individual concerned unless he is advised of the measures taken without his knowledge and thus able retrospectively to challenge their legality. The applicants' main complaint under Article 8 (art. 8) is in fact that the person concerned is not always subsequently informed after the suspension of surveillance and is not therefore in a position to seek an effective remedy before the courts. Their preoccupation is the danger of measures being improperly implemented without the individual knowing or being able to verify the extent to which his rights have been interfered with. In their view, effective control by the courts after the suspension of surveillance measures is necessary in a democratic society to ensure against abuses; otherwise adequate control of secret surveillance is lacking and the right conferred on individuals under Article 8 (art. 8) is simply eliminated. In the Government's view, the subsequent notification which must be given since the Federal Constitutional Court's judgment (see paragraphs 11 and 19 above) corresponds to the requirements of Article 8 para. 2 (art. 8-2). In their submission, the whole efficacy of secret surveillance requires that, both before and after the event, information cannot be divulged if thereby the purpose of the investigation is, or would be retrospectively, thwarted. They stressed that recourse to the courts is no longer excluded after notification has been given, various legal remedies then becoming available to allow the individual, inter alia, to seek redress for any injury suffered (see paragraph 24 above).**

58. **In the opinion of the Court, it has to be ascertained whether it is even feasible in practice to require subsequent notification in all cases. The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore, as the Federal Constitutional Court rightly observed, such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. In the Court's view, in so far as the "interference" resulting from the**

		contested legislation is in principle justified under Article 8 para. 2 (art. 8-2) (see paragraph 48 above), the fact of not informing the individual once surveillance has ceased cannot itself be incompatible with this provision since it is this very fact which ensures the efficacy of the "interference". Moreover, it is to be recalled that, in pursuance of the Federal Constitutional Court's judgment of 15 December 1970, the person concerned must be informed after the termination of the surveillance measures as soon as notification can be made without jeopardising the purpose of the restriction (see paragraphs 11 and 19 above). 59. Both in general and in relation to the question of subsequent notification, the applicants have constantly invoked the danger of abuse as a ground for their contention that the legislation they challenge does not fulfil the requirements of Article 8 para. 2 (art. 8-2) of the Convention. While the possibility of improper action by a dishonest, negligent or over-zealous official can never be completely ruled out whatever the system, the considerations that matter for the purposes of the Court's present review are the likelihood of such action and the safeguards provided to protect against it. **The Court has examined above (at paragraphs 51 to 58) the contested legislation in the light, inter alia, of these considerations. The Court notes in particular that the G 10 contains various provisions designed to reduce the effect of surveillance measures to an unavoidable minimum and to ensure that the surveillance is carried out in strict accordance with the law. In the absence of any evidence or indication that the actual practice followed is otherwise, the Court must assume that in the democratic society of the Federal Republic of Germany, the relevant authorities are properly applying the legislation in issue.** **The Court agrees with the Commission that some compromise between the requirements for defending democratic society and individual rights is inherent in the system of the Convention (see, mutatis mutandis, the judgment of 23 July 1968 in the "Belgian Linguistic" case, Series A no. 6, p. 32, para. 5). As the Preamble to the Convention states, "Fundamental Freedoms ... are best maintained on the one hand by an effective political democracy and on the other by a common understanding and observance of the Human Rights upon which (the Contracting States) depend". In the context of Article 8 (art. 8), this means that a balance must be sought between the exercise by the individual of the right guaranteed to him under paragraph 1 (art. 8-1) and the necessity under paragraph 2 (art. 8-2) to impose secret surveillance for the protection of the democratic society as a whole.** 60. In the light of these considerations and of the detailed examination of the contested legislation, the Court concludes that the German legislature was justified to consider the interference resulting from that legislation with the exercise of the right guaranteed by Article 8 para. 1 (art. 8-1) as being necessary in a democratic society in the interests of national security and for the prevention of disorder or crime (Article 8 para. 2) (art. 8-2). Accordingly, the Court finds no breach of Article 8 (art. 8) of the Convention.
2.	Eur. Court HR, *Malone v. The United Kingdom* judgment of 2 August 1984, 8691/79: interception of postal and telephone	**A. Interception of communications** 2. Whether there was any interference with an Article 8 (art. 8) right 64. **It was common ground that one telephone conversation to which the applicant was a party was intercepted at the request of the police**

	communications; metering; secret surveillance; quality of the law; requirement of foreseeability; adequate protection against arbitrary interference	**under a warrant issued by the Home Secretary (see paragraph 14 above). As telephone conversations are covered by the notions of "private life" and "correspondence" within the meaning of Article 8 (art. 8) (see the Klass and Others judgment of 6 September 1978, Series A no. 28, p. 21, para. 41), the admitted measure of interception involved an "interference by a public authority" with the exercise of a right guaranteed to the applicant under paragraph 1 of Article 8 (art. 8-1).** Despite the applicant's allegations, the Government have consistently declined to disclose to what extent, if at all, his telephone calls and mail have been intercepted otherwise on behalf of the police (see paragraph 16 above). They did, however, concede that, as a suspected receiver of stolen goods, he was a member of a class of persons against whom measures of postal and telephone interception were liable to be employed. As the Commission pointed out in its report (paragraph 115), the existence in England and Wales of laws and practices which permit and establish a system for effecting secret surveillance of communications amounted in itself to an "interference ... with the exercise" of the applicant's rights under Article 8 (art. 8), apart from any measures actually taken against him (see the above-mentioned Klass and Others judgment, ibid.). This being so, the Court, like the Commission (see the report, paragraph 114), does not consider it necessary to inquire into the applicant's further claims that both his mail and his telephone calls were intercepted for a number of years. 3. Whether the interferences were justified 65. The principal issue of contention was whether the interferences found were justified under the terms of paragraph 2 of Article 8 (art. 8-2), notably whether they were "in accordance with the law" and "necessary in a democratic society" for one of the purposes enumerated in that paragraph. (a) "In accordance with the law" *(i) General principles* 66. **The Court held in its Silver and Others judgment of 25 March 1983 (Series A no. 61, pp. 32-33, para. 85) that, at least as far as interferences with prisoners' correspondence were concerned, the expression "in accordance with the law/prévue par la loi" in paragraph 2 of Article 8 (art. 8-2) should be interpreted in the light of the same general principles as were stated in the Sunday Times judgment of 26 April 1979 (Series A no. 30) to apply to the comparable expression "prescribed by law/ prévues par la loi" in paragraph 2 of Article 10 (art. 10-2). The first such principle was that the word "law/loi" is to be interpreted as covering not only written law but also unwritten law (see the abovementioned Sunday Times judgment, p. 30, para. 47). A second principle, recognised by Commission, Government and applicant as being applicable in the present case, was that "the interference in question must have some basis in domestic law" (see the the above-mentioned Silver and Others judgment, p. 33, para. 86). The expressions in question were, however, also taken to include requirements over and above compliance with the domestic law. Two of these requirements were explained in the following terms: "Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as 'law' unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able - if need be with appropriate advice - to**

foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail." (Sunday Times judgment, p. 31, para. 49; Silver and Others judgment, p. 33, paras. 87 and 88)

67. In the Government's submission, these two requirements, which were identified by the Court in cases concerning the imposition of penalties or restrictions on the exercise by the individual of his right to freedom of expression or to correspond, are less appropriate in the wholly different context of secret surveillance of communications. In the latter context, where the relevant law imposes no restrictions or controls on the individual to which he is obliged to conform, the paramount consideration would appear to the Government to be the lawfulness of the administrative action under domestic law. **The Court would reiterate its opinion that the phrase "in accordance with the law" does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention (see, mutatis mutandis, the above-mentioned Silver and Others judgment, p. 34, para. 90, and the Golder judgment of 21 February 1975, Series A no. 18, p. 17, para. 34). The phrase thus implies - and this follows from the object and purpose of Article 8 (art. 8) - that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by paragraph 1 (art. 8-1) (see the report of the Commission, paragraph 121). Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident (see the abovementioned Klass and Others judgment, Series A no. 28, pp. 21 and 23, paras. 42 and 49). Undoubtedly, as the Government rightly suggested, the requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.**

68. **There was also some debate in the pleadings as to the extent to which, in order for the Convention to be complied with, the "law" itself, as opposed to accompanying administrative practice, should define the circumstances in which and the conditions on which a public authority may interfere with the exercise of the protected rights. The above-mentioned judgment in the case of Silver and Others, which was delivered subsequent to the adoption of the Commission's report in the present case, goes some way to answering the point. In that judgment, the Court held that "a law which confers a discretion must indicate the scope of that discretion", although the detailed procedures and conditions to be observed do not necessarily have to be incorporated in rules of substantive law (ibid., Series A no. 61, pp. 33-34, paras. 88-89). The degree of precision required of the "law" in this connection will depend upon the particular subject-matter (see the above-mentioned Sunday Times judgment, Series A no. 30, p. 31, para. 49). Since the implementation in practice of measures of secret**

surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.

(ii) Application in the present case of the foregoing principles

79. The foregoing considerations disclose that, at the very least, in its present state the law in England and Wales governing interception of communications for police purposes is somewhat obscure and open to differing interpretations. The Court would be usurping the function of the national courts were it to attempt to make an authoritative statement on such issues of domestic law (see, mutatis mutandis, the Deweer judgment of 27 February 1980, Series A no. 35, p. 28, in fine, and the Van Droogenbroeck judgment of 24 June 1982, Series A no. 50, p. 30, fourth sub-paragraph). The Court is, however, required under the Convention to determine whether, for the purposes of paragraph 2 of Article 8 (art. 8-2), the relevant law lays down with reasonable clarity the essential elements of the authorities' powers in this domain. Detailed procedures concerning interception of communications on behalf of the police in England and Wales do exist (see paragraphs 42-49, 51-52 and 54-55 above). What is more, published statistics show the efficacy of those procedures in keeping the number of warrants granted relatively low, especially when compared with the rising number of indictable crimes committed and telephones installed (see paragraph 53 above). The public have been made aware of the applicable arrangements and principles through publication of the Birkett report and the White Paper and through statements by responsible Ministers in Parliament (see paragraphs 21, 37-38, 41, 43 and 54 above). Nonetheless, on the evidence before the Court, it cannot be said with any reasonable certainty what elements of the powers to intercept are incorporated in legal rules and what elements remain within the discretion of the executive. In view of the attendant obscurity and uncertainty as to the state of the law in this essential respect, the Court cannot but reach a similar conclusion to that of the Commission. **In the opinion of the Court, the law of England and Wales does not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities. To that extent, the minimum degree of legal protection to which citizens are entitled under the rule of law in a democratic society is lacking.**

(iii) Conclusion

80. In sum, as far as interception of communications is concerned, the interferences with the applicant's right under Article 8 (art. 8) to respect for his private life and correspondence (see paragraph 64 above) were not "in accordance with the law".

(b) "Necessary in a democratic society" for a recognised purpose

81. **Undoubtedly, the existence of some law granting powers of interception of communications to aid the police in their function of investigating and detecting crime may be "necessary in a democratic society ... for the prevention of disorder or crime", within the meaning of paragraph 2 of Article 8 (art. 8-2) (see, mutatis mutandis, the above-mentioned Klass and Others judgment, Series A no. 28, p.**

23, para. 48). The Court accepts, for example, the assertion in the Government's White Paper (at para. 21) that in Great Britain "the increase of crime, and particularly the growth of organised crime, the increasing sophistication of criminals and the ease and speed with which they can move about have made telephone interception an indispensable tool in the investigation and prevention of serious crime". However, the exercise of such powers, because of its inherent secrecy, carries with it a danger of abuse of a kind that is potentially easy in individual cases and could have harmful consequences for democratic society as a whole (ibid., p. 26, para. 56). This being so, the resultant interference can only be regarded as "necessary in a democratic society" if the particular system of secret surveillance adopted contains adequate guarantees against abuse (ibid., p. 23, paras. 49-50).

82. The applicant maintained that the system in England and Wales for the interception of postal and telephone communications on behalf of the police did not meet this condition. In view of its foregoing conclusion that the interferences found were not "in accordance with the law", the Court considers that it does not have to examine further the content of the other guarantees required by paragraph 2 of Article 8 (art. 8-2) and whether the system circumstances.

B. Metering

83. **The process known as "metering" involves the use of a device (a meter check printer) which registers the numbers dialled on a particular telephone and the time and duration of each call (see paragraph 56 above). In making such records, the Post Office - now British Telecommunications - makes use only of signals sent to itself as the provider of the telephone service and does not monitor or intercept telephone conversations at all. From this, the Government drew the conclusion that metering, in contrast to interception of communications, does not entail interference with any right guaranteed by Article 8 (art. 8).**

84. **As the Government rightly suggested, a meter check printer registers information that a supplier of a telephone service may in principle legitimately obtain, notably in order to ensure that the subscriber is correctly charged or to investigate complaints or possible abuses of the service. By its very nature, metering is therefore to be distinguished from interception of communications, which is undesirable and illegitimate in a democratic society unless justified. The Court does not accept, however, that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Article 8 (art. 8). The records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8 (art. 8).**

87. Section 80 of the Post Office Act 1969 has never been applied so as to "require" the Post Office, pursuant to a warrant of the Secretary of State, to make available to the police in connection with the investigation of crime information obtained from metering. On the other hand, no rule of domestic law makes it unlawful for the Post Office voluntarily to comply with a request from the police to make and supply records of metering (see paragraph 56 above). The practice described above, including the

		limitative conditions as to when the information may be provided, has been made public in answer to parliamentary questions (ibid.). **However, on the evidence adduced before the Court, apart from the simple absence of prohibition, there would appear to be no legal rules concerning the scope and manner of exercise of the discretion enjoyed by the public authorities. Consequently, although lawful in terms of domestic law, the interference resulting from the existence of the practice in question was not "in accordance with the law", within the meaning of paragraph 2 of Article 8 (art. 8-2) (see paragraphs 66 to 68 above).** 89. There has accordingly been a breach of Article 8 (art. 8) in the applicant's case as regards both interception of communications and release of records of metering to the police.
3.	Eur. Court HR, *Leander v. Sweden* judgment of 26 March 1987, 9248/81: storage in secret registers; legitimate aims; interests of national security; adequate and effective guarantees against abuse	**A. Whether there was any interference with an Article 8 (art. 8) right** 48. It is uncontested that the secret police-register contained information relating to Mr. Leander's private life. Both the storing and the release of such information, which were coupled with a refusal to allow Mr. Leander an opportunity to refute it, amounted to an interference with his right to respect for private life as guaranteed by Article 8 § 1 (art. 8-1). **B. Whether the interference was justified** 1. Legitimate aim 49. The aim of the Swedish personnel control system is clearly a legitimate one for the purposes of Article 8 (art. 8), namely the protection of national security. The main issues of contention were whether the interference was "in accordance with the law" and "necessary in a democratic society". 2. "In accordance with the law" *(a) General principles* 50. **The expression "in accordance with the law" in paragraph 2 of Article 8 (art. 8-2) requires, to begin with, that the interference must have some basis in domestic law. Compliance with domestic law, however, does not suffice: the law in question must be accessible to the individual concerned and its consequences for him must also be foreseeable (see, mutatis mutandis, the Malone judgment of 2 August 1984, Series A no. 82, pp. 31-32, § 66).** 51. **However, the requirement of foreseeability in the special context of secret controls of staff in sectors affecting national security cannot be the same as in many other fields. Thus, it cannot mean that an individual should be enabled to foresee precisely what checks will be made in his regard by the Swedish special police service in its efforts to protect national security. Nevertheless, in a system applicable to citizens generally, as under the Personnel Control Ordinance, the law has to be sufficiently clear in its terms to give them an adequate indication as to the circumstances in which and the conditions on which the public authorities are empowered to resort to this kind of secret and potentially dangerous interference with private life (ibid., p. 32, § 67). In assessing whether the criterion of foreseeability is satisfied, account may be taken also of instructions or administrative practices which do not have the status of substantive law, in so far as those concerned are made sufficiently aware of their contents (see the Silver and Others judgment of 25 March 1983, Series A no. 61, pp. 33-34, §§ 88-89). In addition, where the implementation of the law**

consists of secret measures, not open to scrutiny by the individuals concerned or by the public at large, the law itself, as opposed to the accompanying administrative practice, must indicate the scope of any discretion conferred on the competent authority with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference (see the above-mentioned Malone judgment, Series A no. 82, pp. 32-33, § 68).

(b) Application in the present case of the foregoing principles

52. The interference had a valid basis in domestic law, namely the Personnel Control Ordinance. However, the applicant claimed that the provisions governing the keeping of the secret policeregister, that is primarily section 2 of the Ordinance, lacked the required accessibility and foreseeability. Both the Government and the Commission disagreed with this contention.

53. The Ordinance itself, which was published in the Swedish Official Journal, doubtless meets the requirement of accessibility. The main question is thus whether domestic law laid down, with sufficient precision, the conditions under which the National Police Board was empowered to store and release information under the personnel control system.

54. The first paragraph of section 2 of the Ordinance does confer a wide discretion on the National Police Board as to what information may be entered in the register (see paragraph 19 above). The scope of this discretion is however limited by law in important respects through the second paragraph, which corresponds to the prohibition already contained in the Constitution (see paragraph 18 above), in that "no entry is allowed merely for the reason that a person, by belonging to an organisation or by other means, has expressed a political opinion". In addition, the Board's discretion in this connection is circumscribed by instructions issued by the Government (see paragraphs 20-21 above). However, of these only one is public and hence sufficiently accessible to be taken into account, namely the Instruction of 22 September 1972 (see paragraph 20 above). The entering of information on the secret police-register is also subject to the requirements that the information be necessary for the special police service and be intended to serve the purpose of preventing or detecting "offences against national security, etc." (first paragraph of section 2 of the Ordinance - see paragraph 19 above)

55. Furthermore, the Ordinance contains explicit and detailed provisions as to what information may be handed out, the authorities to which information may be communicated, the circumstances in which such communication may take place and the procedure to be followed by the National Police Board when taking decisions to release information (see paragraphs 25-29 above).

56. Having regard to the foregoing, **the Court finds that Swedish law gives citizens an adequate indication as to the scope and the manner of exercise of the discretion conferred on the responsible authorities to collect, record and release information under the personnel control system.**

57. The interference in the present case with Mr. Leander's private life was therefore "in accordance with the law", within the meaning of Article 8 (art. 8).

3. "Necessary in a democratic society in the interests of national security"

58. **The notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued (see, inter alia, the Gillow judgment of 24 November 1986, Series A no. 109, p. 22, § 55).**

59. **However, the Court recognises that the national authorities enjoy a margin of appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved. In the instant case, the interest of the respondent State in protecting its national security must be balanced against the seriousness of the interference with the applicant's right to respect for his private life. There can be no doubt as to the necessity, for the purpose of protecting national security, for the Contracting States to have laws granting the competent domestic authorities power, firstly, to collect and store in registers not accessible to the public information on persons and, secondly, to use this information when assessing the suitability of candidates for employment in posts of importance for national security. Admittedly, the contested interference adversely affected Mr. Leander's legitimate interests through the consequences it had on his possibilities of access to certain sensitive posts within the public service. On the other hand, the right of access to public service is not as such enshrined in the Convention (see, inter alia, the Kosiek judgment of 28 August 1986, Series A no. 105, p. 20, §§ 34- 35), and, apart from those consequences, the interference did not constitute an obstacle to his leading a private life of his own choosing. In these circumstances, the Court accepts that the margin of appreciation available to the respondent State in assessing the pressing social need in the present case, and in particular in choosing the means for achieving the legitimate aim of protecting national security, was a wide one.**

60. **Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security poses of undermining or even destroying democracy on the ground of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse (see the Klass and Others judgment of 6 September 1978, Series A no. 28, pp. 23-24, §§ 49-50).**

61. The applicant maintained that such guarantees were not provided to him under the Swedish personnel control system, notably because he was refused any possibility of challenging the correctness of the information concerning him.

62. The Government invoked twelve different safeguards, which, in their opinion, provided adequate protection when taken together: (i) the existence of personnel control as such is made public through the Personnel Control Ordinance; (ii) there is a division of sensitive posts into different security classes (see paragraph 26 above); (iii) only relevant information may be collected and released (see paragraphs 18-20, 28 and 30 above); (iv) a request for information may be made only with regard to the person whom it is intended to appoint (see paragraph 27 above); (v) parliamentarians are members of the National Police Board (see paragraph 29 above); (vi) information may be communicated to the person in question; the Government did, however, concede that no such communication had ever been made, at least under the provisions in force before 1 October 1983 (see paragraph 31 above); (vii) the decision

whether or not to appoint the person in question rests with the requesting authority and not with the National Police Board (see paragraph 34 above); (viii) an appeal against this decision can be lodged with the Government (see paragraph 16 above); (ix) the supervision effected by the Minister of Justice (see paragraph 35 above); (x) the supervision effected by the Chancellor of Justice (see paragraphs 36-37 above); (xi) the supervision effected by the Parliamentary Ombudsman (see paragraphs 38-39 above); (xii) the supervision effected by the Parliamentary Committee on Justice (see paragraph 40 above).

63. The Court first points out that some of these safeguards are irrelevant in the present case, since, for example, there was never any appealable appointment decision (see paragraphs 11 and 16 above).

64. The Personnel Control Ordinance contains a number of provisions designed to reduce the effects of the personnel control procedure to an unavoidable minimum (see notably paragraphs 54-55 and nos. (ii)-(iv) in paragraph 62 above). Furthermore, the use of the information on the secret police-register in areas outside personnel control is limited, as a matter of practice, to cases of public prosecution and cases concerning the obtaining of Swedish citizenship (see paragraph 22 above). The supervision of the proper implementation of the system is, leaving aside the controls exercised by the Government themselves, entrusted both to Parliament and to independent institutions (see paragraphs 35-40 above).

65. The Court attaches particular importance to the presence of parliamentarians on the National Police Board and to the supervision effected by the Chancellor of Justice and the Parliamentary Ombudsman as well as the Parliamentary Committee on Justice (see paragraph 62 above, nos. (v), (x), (xi) and (xii)). The parliamentary members of the Board, who include members of the Opposition (see paragraph 29 above), participate in all decisions regarding whether or not information should be released to the requesting authority. In particular, each of them is vested with a right of veto, the exercise of which automatically prevents the Board from releasing the information. In such a case, a decision to release can be taken only by the Government themselves and then only if the matter has been referred to them by the National Police Commissioner or at the request of one of the parliamentarians (see paragraph 29 above). This direct and regular control over the most important aspect of the register - the release of information - provides a major safeguard against abuse. In addition, a scrutiny is effected by the Parliamentary Committee on Justice (see paragraph 40 above). The supervision carried out by the Parliamentary Ombudsman constitutes a further significant guarantee against abuse, especially in cases where individuals feel that their rights and freedoms have been encroached upon (see paragraphs 38-39 above). As far as the Chancellor of Justice is concerned, it may be that in some matters he is the highest legal adviser of the Government. However, it is the Swedish Parliament which has given him his mandate to supervise, amongst other things, the functioning of the personnel control system. In doing so, he acts in much the same way as the Ombudsman and is, at least in practice, independent of the Government (see paragraphs 36-37 above).

66. The fact that the information released to the military authorities was not communicated to Mr. Leander cannot by itself warrant the conclusion that the interference was not "necessary in a democratic society in the interests of national security", as it is the very absence of such communication which, at least partly, ensures the efficacy of the personnel control procedure (see, mutatis mutandis, the above-mentioned Klass and Others judgment, Series A no. 28, p. 27, § 58). The Court notes, however, that various authorities consulted before the issue of the Ordinance of

		1969, including the Chancellor of Justice and the Parliamentary Ombudsman, considered it desirable that the rule of communication to the person concerned, as contained in section 13 of the Ordinance, should be effectively applied in so far as it did not jeopardise the purpose of the control (see paragraph 31 above). 67. **The Court, like the Commission, thus reaches the conclusion that the safeguards contained in the Swedish personnel control system meet the requirements of paragraph 2 of Article 8 (art. 8-2). Having regard to the wide margin of appreciation available to it, the respondent State was entitled to consider that in the present case the interests of national security prevailed over the individual interests of the applicant (see paragraph 59 above). The interference to which Mr. Leander was subjected cannot therefore be said to have been disproportionate to the legitimate aim pursued.** 68. Accordingly, there has been no breach of Article 8 (art. 8).
4.	Eur. Court HR, *Kruslin v. France* judgment of 24 April 1990, 11801/85; and Eur. Court HR, *Huvig v. France* judgment of 24 April 1990, 11105/84: interception of communications; telephone tapping; secret surveillance; adequate safeguards against abuses; minimum degree of protection	27. **The expression "in accordance with the law", within the meaning of Article 8 § 2 (art. 8-2), requires firstly that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and compatible with the rule of law.** 29. **Like the Government and the Delegate, the Court points out, firstly, that it is primarily for the national authorities, notably the courts, to interpret and apply domestic law (see, among many other authorities, the Malone judgment previously cited, Series A no. 82, p. 36, § 79, and the Eriksson judgment of 22 June 1989, Series A no. 156, p. 25, § 62). It is therefore not for the Court to express an opinion contrary to theirs on whether telephone tapping ordered by investigating judges is compatible with Article 368 of the Criminal Code. For many years now, the courts - and in particular the Court of Cassation - have regarded Articles 81, 151 and 152 of the Code of Criminal Procedure as providing a legal basis for telephone tapping carried out by a senior police officer (officier de police judiciaire) under a warrant issued by an investigating judge.** **Settled case-law of this kind cannot be disregarded. In relation to paragraph 2 of Article 8 (art. 8-2) of the Convention and other similar clauses, the Court has always understood the term "law" in its "substantive" sense, not its "formal" one; it has included both enactments of lower rank than statutes (see, in particular, the De Wilde, Ooms and Versyp judgment of 18 June 1971, Series A no. 12, p. 45, § 93) and unwritten law. The Sunday Times, Dudgeon and Chappell judgments admittedly concerned the United Kingdom, but it would be wrong to exaggerate the distinction between common-law countries and Continental countries, as the Government rightly pointed out. Statute law is, of course, also of importance in common-law countries. Conversely, case-law has traditionally played a major role in Continental countries, to such an extent that whole branches of positive law are largely the outcome of decisions by the courts. The Court has indeed taken account of case-law in such countries on more than one occasion (see, in particular, the Müller and Others judgment of 24 May 1988, Series A no. 133, p. 20, § 29, the Salabiaku judgment of 7 October 1988, Series A no. 141, pp. 16-17, § 29, and the Markt Intern Verlag GmbH and Klaus Beermann judgment of 20 November 1989, Series A no. 165, pp. 18-19, § 30). Were it to overlook case-law, the Court would undermine the legal system of the Continental States almost as much as the Sunday Times judgment**

of 26 April 1979 would have "struck at the very roots" of the United Kingdom's legal system if it had excluded the common law from the concept of "law" (Series A no. 30, p. 30, § 47). In a sphere covered by the written law, the "law" is the enactment in force as the competent courts have interpreted it in the light, if necessary, of any new practical developments.
In sum, the interference complained of had a legal basis in French law.

30. **The second requirement which emerges from the phrase "in accordance with the law" - the accessibility of the law - does not raise any problem in the instant case. The same is not true of the third requirement, the law's "foreseeability" as to the meaning and nature of the applicable measures. As the Court pointed out in the Malone judgment of 2 August 1984, Article 8 § 2 (art. 8-2) of the Convention "does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law". It "thus implies ... that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by paragraph 1 (art. 8-1) ... Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident ... Undoubtedly ..., the requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations" - or judicial investigations - "as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.... [In its judgment of 25 March 1983 in the case of Silver and Others the Court] held that 'a law which confers a discretion must indicate the scope of that discretion', although the detailed procedures and conditions to be observed do not necessarily have to be incorporated in rules of substantive law (ibid., Series A no. 61, pp. 33-34, §§ 88-89). The degree of precision required of the 'law' in this connection will depend upon the particular subject-matter ... Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive" - or to a judge - "to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity ... to give the individual adequate protection against arbitrary interference." (Series A no. 82, pp. 32-33, §§ 67-68)**

31. **The Government submitted that the Court must be careful not to rule on whether French legislation conformed to the Convention in the abstract and not to give a decision based on legislative policy. The Court was therefore not concerned, they said, with matters irrelevant to Mr Kruslin's case, such as the possibility of telephone tapping in relation to minor offences or the fact that there was no requirement that an individual whose telephone had been monitored should be so informed after the event where proceedings**

had not in the end been taken against him. Such matters were in reality connected with the condition of "necessity in a democratic society", fulfilment of which had to be reviewed in concrete terms, in the light of the particular circumstances of each case.

32. **The Court is not persuaded by this argument. Since it must ascertain whether the interference complained of was "in accordance with the law", it must inevitably assess the relevant French "law" in force at the time in relation to the requirements of the fundamental principle of the rule of law. Such a review necessarily entails some degree of abstraction. It is none the less concerned with the "quality" of the national legal rules applicable to Mr Kruslin in the instant case.**

33. **Tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated.**
Before the Commission (supplementary observations of 4 July 1988, pages 4-7, summarised in paragraph 37 of the report) and, in a slightly different form, before the Court, the Government listed seventeen safeguards which they said were provided for in French law (droit). These related either to the carrying out of telephone tapping or to the use made of the results or to the means of having any irregularities righted, and the Government claimed that the applicant had not been deprived of any of them.

34. The Court does not in any way minimise the value of several of the safeguards, in particular the need for a decision by an investigating judge, who is an independent judicial authority; the latter's supervision of senior police officers and the possible supervision of the judge himself by the Indictment Division, by trial courts and courts of appeal and, if need be, by the Court of Cassation; the exclusion of any "subterfuge" or "ruse" consisting not merely in the use of telephone tapping but in an actual trick, trap or provocation; and the duty to respect the confidentiality of relations between suspect or accused and lawyer.
It has to be noted, however, that only some of these safeguards are expressly provided for in Articles 81, 151 and 152 of the Code of Criminal Procedure. Others have been laid down piecemeal in judgments given over the years, the great majority of them after the interception complained of by Mr Kruslin (June 1982). Some have not yet been expressly laid down in the case-law at all, at least according to the information gathered by the Court; the Government appear to infer them either from general enactments or principles or else from an analogical interpretation of legislative provisions - or court decisions - concerning investigative measures different from telephone tapping, notably searches and seizure of property. Although plausible in itself, such "extrapolation" does not provide sufficient legal certainty in the present context.

35. **Above all, the system does not for the time being afford adequate safeguards against various possible abuses. For example, the categories of people liable to have their telephones tapped by judicial order and the nature of the offences which may give rise to such an order are nowhere defined. Nothing obliges a judge to set a limit on the duration of telephone tapping. Similarly unspecified are the procedure for drawing up the summary reports containing intercepted conversations; the precautions to be taken in order to communicate the recordings intact and in their entirety for possible**

		inspection by the judge (who can hardly verify the number and length of the original tapes on the spot) and by the defence; and the circumstances in which recordings may or must be erased or the tapes be destroyed, in particular where an accused has been discharged by an investigating judge or acquitted by a court. The information provided by the Government on these various points shows at best the existence of a practice, but a practice lacking the necessary regulatory control in the absence of legislation or case-law. 36. **In short, French law, written and unwritten, does not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities**. This was truer still at the material time, so that Mr Kruslin did not enjoy the **minimum degree of protection to which citizens are entitled under the rule of law in a democratic society** (see the Malone judgment previously cited, Series A no. 82, p. 36, § 79). There has therefore been a breach of Article 8 (art. 8) of the Convention.
5.	Eur. Court HR, *Lüdi v. Switzerland*, judgment of 15 June 1992, 12433/86: telephone interception; national security; criminal offences; prevention of crime	39. **There is no doubt that the telephone interception was an interference with Mr Lüdi's private life and correspondence. Such an interference is not in breach of the Convention if it complies with the requirements of paragraph 2 of Article 8 (art. 8-2).** On this point the Court is in agreement with the Commission. The measure in question was based on Articles 171b and 171c of the Berne Code of Criminal Procedure, which apply - as the Federal Court found (see paragraph 21 above) - even to the preliminary stage of an investigation, where there is good reason to believe that criminal offences are about to be committed. Moreover, it was aimed at the "prevention of crime", and the Court has no doubt whatever as to its necessity in a democratic society. 40. **On the other hand, the Court agrees with the Government that in the present case the use of an undercover agent did not, either alone or in combination with the telephone interception, affect private life within the meaning of Article 8 (art. 8). Toni's actions took place within the context of a deal relating to 5 kg of cocaine. The cantonal authorities, who had been warned by the German police, selected a sworn officer to infiltrate what they thought was a large network of traffickers intending to dispose of that quantity of drugs in Switzerland. The aim of the operation was to arrest the dealers when the drugs were handed over. Toni thereupon contacted the applicant, who said that he was prepared to sell him 2 kg of cocaine, worth 200,000 Swiss francs (see paragraphs 9 and 13 above). Mr Lüdi must therefore have been aware from then on that he was engaged in a criminal act punishable under Article 19 of the Drugs Law and that consequently he was running the risk of encountering an undercover police officer whose task would in fact be to expose him.** 41. In short, there was no violation of Article 8 (art. 8).
6.	Eur. Court HR, *Niemietz v. Germany* judgment of 16 December 1992, 13710/88: telephone tapping; business activities; professional secrecy; necessary in a democratic society;	29. **The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of "private life". However, it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings.** **There appears, furthermore, to be no reason of principle why this**

	proportionate to the legitimate aim	**understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world. This view is supported by the fact that, as was rightly pointed out by the Commission, it is not always possible to distinguish clearly which of an individual's activities form part of his professional or business life and which do not. Thus, especially in the case of a person exercising a liberal profession, his work in that context may form part and parcel of his life to such a degree that it becomes impossible to know in what capacity he is acting at a given moment of time.** **To deny the protection of Article 8 (art. 8) on the ground that the measure complained of related only to professional activities - as the Government suggested should be done in the present case - could moreover lead to an inequality of treatment, in that such protection would remain available to a person whose professional and non-professional activities were so intermingled that there was no means of distinguishing between them. In fact, the Court has not heretofore drawn such distinctions: it concluded that there had been an interference with private life even where telephone tapping covered both business and private calls (see the Huvig v. France judgment of 24 April 1990, Series A no. 176-B, p. 41, para. 8, and p. 52, para. 25); and, where a search was directed solely against business activities, it did not rely on that fact as a ground for excluding the applicability of Article 8 (art. 8) under the head of "private life" (see the Chappell v. the United Kingdom judgment of 30 March 1989, Series A no. 152-A, pp. 12-13, para. 26, and pp. 21-22, para. 51.)** 30. **As regards the word "home", appearing in the English text of Article 8 (art. 8), the Court observes that in certain Contracting States, notably Germany (see paragraph 18 above), it has been accepted as extending to business premises. Such an interpretation is, moreover, fully consonant with the French text, since the word "domicile" has a broader connotation than the word "home" and may extend, for example, to a professional person's office.** **In this context also, it may not always be possible to draw precise distinctions, since activities which are related to a profession or business may well be conducted from a person's private residence and activities which are not so related may well be carried on in an office or commercial premises. A narrow interpretation of the words "home" and "domicile" could therefore give rise to the same risk of inequality of treatment as a narrow interpretation of the notion of "private life" (see paragraph 29 above).** 31. **More generally, to interpret the words "private life" and "home" as including certain professional or business activities or premises would be consonant with the essential object and purpose of Article 8 (art. 8), namely to protect the individual against arbitrary interference by the public authorities (see, for example, the Marckx v. Belgium judgment of 13 June 1979, Series A no. 31, p. 15, para. 31). Such an interpretation would not unduly hamper the Contracting States, for they would retain their entitlement to "interfere" to the extent permitted by paragraph 2 of Article 8 (art. 8-2); that entitlement might well be more far-reaching where professional or business activities or premises were involved than would otherwise be the case.** 32. To the above-mentioned general considerations, which militate against the view that Article 8 (art. 8) is not applicable, must be added a

		further factor pertaining to the particular circumstances of the case. The warrant issued by the Munich District Court ordered a search for, and seizure of, "documents" - without qualification or limitation - revealing the identity of Klaus Wegner (see paragraph 10 above). Furthermore, those conducting the search examined four cabinets with data concerning clients as well as six individual files (see paragraph 11 above); their operations must perforce have covered "correspondence" and materials that can properly be regarded as such for the purposes of Article 8 (art. 8). In this connection, it is sufficient to note that that provision does not use, as it does for the word "life", any adjective to qualify the word "correspondence". And, indeed, the Court has already held that, in the context of correspondence in the form of telephone calls, no such qualification is to be made (see the above-mentioned Huvig judgment, Series A no. 176-B, p. 41, para. 8, and p. 52, para. 25). Again, in a number of cases relating to correspondence with a lawyer (see, for example, the Schönenberger and Durmaz v. Switzerland judgment of 20 June 1988, Series A no. 137, and the Campbell v. the United Kingdom judgment of 25 March 1992, Series A no. 233), the Court did not even advert to the possibility that Article 8 (art. 8) might be inapplicable on the ground that the correspondence was of a professional nature. 33. Taken together, the foregoing reasons lead **the Court to find that the search of the applicant's office constituted an interference with his rights under Article 8 (art. 8).** 37. **As to whether the interference was "necessary in a democratic society", the Court inclines to the view that the reasons given therefor by the Munich District Court (see paragraph 10 above) can be regarded as relevant in terms of the legitimate aims pursued. It does not, however, consider it essential to pursue this point since it has formed the opinion that, as was contended by the applicant and as was found by the Commission, the measure complained of was not proportionate to those aims.** It is true that the offence in connection with which the search was effected, involving as it did not only an insult to but also an attempt to bring pressure on a judge, cannot be classified as no more than minor. On the other hand, the warrant was drawn in broad terms, in that it ordered a search for and seizure of "documents", without any limitation, revealing the identity of the author of the offensive letter; this point is of special significance where, as in Germany, the search of a lawyer's office is not accompanied by any special procedural safeguards, such as the presence of an independent observer. More importantly, having regard to the materials that were in fact inspected, the search impinged on professional secrecy to an extent that appears disproportionate in the circumstances; it has, in this connection, to be recalled that, where a lawyer is involved, an encroachment on professional secrecy may have repercussions on the proper administration of justice and hence on the rights guaranteed by Article 6 (art. 6) of the Convention. In addition, the attendant publicity must have been capable of affecting adversely the applicant's professional reputation, in the eyes both of his existing clients and of the public at large.
7.	Eur. Court HR, *Murray v. The United Kingdom* judgment of 28 October 1994, 14310/88: prevention of terrorism; national security; proportionate to the	90. **It remains to be determined whether they were necessary in a democratic society and, in particular, whether the means employed were proportionate to the legitimate aim pursued. In this connection it is not for the Court to substitute for the assessment of the national authorities its own assessment of what might be the best policy in the field of investigation of terrorist crime (see the above-mentioned Klass and Others judgment, p. 23, para. 49). A certain margin of appreciation in deciding what measures to take both in general and**

	legitimate aim; necessary in a democratic society	**in particular cases should be left to the national authorities.** 91. **The present judgment has already adverted to the responsibility of an elected government in a democratic society to protect its citizens and its institutions against the threats posed by organized terrorism and to the special problems involved in the arrest and detention of persons suspected of terrorist-linked offences (see paragraphs 47, 51 and 58 above). These two factors affect the fair balance that is to be struck between the exercise by the individual of the right guaranteed to him or her under paragraph 1 of Article 8 (art. 8-1) and the necessity under paragraph 2 (art. 8-2) for the State to take effective measures for the prevention of terrorist crimes (see, mutatis mutandis, the above-mentioned Klass and Others judgment, p. 28, para. 59).** 92. The domestic courts held that Mrs Murray was genuinely and honestly suspected of the commission of a terrorist-linked crime (see paragraphs 24 and 28 above). The European Court, for its part, has found on the evidence before it that this suspicion could be regarded as reasonable for the purposes of sub-paragraph (c) Article 5 para. 1 (art. 5-1-c) (see paragraph 63 above). The Court accepts that there was in principle a need both for powers of the kind granted by section 14 of the 1978 Act and, in the particular case, to enter and search the home of the Murray family in order to arrest Mrs Murray. Furthermore, the "conditions of extreme tension", as Lord Griffiths put it in his speech in the House of Lords, under which such arrests in Northern Ireland have to be carried out must be recognised. The Court notes the analysis of Lord Griffiths, when he said (see paragraph 33 above): "The search cannot be limited solely to looking for the person to be arrested and must also embrace a search whose object is to secure that the arrest should be peaceable. I ... regard it as an entirely reasonable precaution that all the occupants of the house should be asked to assemble in one room. ... It is in everyone's best interest that the arrest is peaceably effected and I am satisfied that the procedures adopted by the Army are sensible, reasonable and designed to bring about the arrest with the minimum of danger and distress to all concerned." These are legitimate considerations which go to explain and justify the manner in which the entry into and search of the applicants' home were carried out. **The Court does not find that, in relation to any of the applicants, the means employed by the authorities in this regard were disproportionate to the aim pursued.** 93. Neither can it be regarded as falling outside the legitimate bounds of the process of investigation of terrorist crime for the competent authorities to record and retain basic personal details concerning the arrested person or even other persons present at the time and place of arrest. None of the personal details taken during the search of the family home or during Mrs Murray's stay at the Army centre would appear to have been irrelevant to the procedures of arrest and interrogation (see paragraphs 12 to 15 above). Similar conclusions apply to the taking and retention of a photograph of Mrs Murray at the Army centre (see paragraphs 13 and 14 above). In this connection too, the Court does not find that the means employed were disproportionate to the aim pursued. 94. In the light of the particular facts of the case, the Court finds that the various measures complained of can be regarded as having been necessary in a democratic society for the prevention of crime, within the meaning of Article 8 para. 2 (art. 8-2).
8.	Eur. Court HR, *Friedl v.*	**Report of the European Commission of Human Rights**

	Austria judgment of 25 January 1995, 15225/89: storing and release of information; photographs; secret register; identification; necessary in a democratic society; prevention of disorder and crime	44. **The Commission recalls that the notion of "private life" is not limited to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within this circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings and the outside world (Eur. Court H.R., Niemietz judgment of 16 December 1992, Series A No. 251-B, p. 33, para. 29; see also No. 3868/68, Dec. 25.5.70, Coll. 34 p. 10; No. 6825/75, 18.5.76, D.R. 5 p. 86; Brüggemann and Scheuten v. Germany, Comm. Report 12.7.77, paras. 55-58, D.R. 10 p. 100).** 46. **In the case-law of the Convention organs, both the storing and release of information relating to an individual's private life in a secret police register have been found to constitute an interference with the person's right to respect for his private life (Eur. Court H.R., Leander judgment of 26 March 1987, Series A no. 116, p. 22, para. 48). Furthermore, a compulsory public census, including questions relating to personal details of the inhabitants of a particular household, or the requirement, pursuant to the relevant tax legislation, to produce a list of one's private expenditure amount to such an interference (cf. No. 9702/82, Dec. 6.10.82, D.R. 30 p. 239; No. 9804/82, Dec. 7.12.82, D.R. 31 p. 231). The examination of a person in the course of his detention, including measures such as his search, questioning about his private life, taking of fingerprints and photographs, and the retention of the records of this examination, was also regarded as interference with the person's right to respect for his private life (cf. McVeigh, O'Neill, Evans v. United Kingdom, Comm. Report 18.3.81, D.R. 25 p. 15, para. 224).** <u>a. Taking of photographs and their retention</u> 48. **For the purpose of delimiting the scope of the protection afforded by Article 8 (Art. 8) of the Convention against arbitrary interference by public authorities, the Commission has attached importance to the questions whether the taking of photographs amounted to an intrusion into the individual's privacy, whether it related to private matters or public incidents, and whether the material thus obtained was envisaged for a limited use or was likely to be made available to the general public (No. 5877/72, Dec. 12.10.72, Yearbook 16 p. 328). Furthermore, the Commission did not regard the use of individual photographs in the course of a criminal investigation as such an interference, where the photographs concerned had either been previously provided voluntarily in connection with applications for official documents, or had been obtained on the occasion of a previous arrest, and were not made available to the general public nor used for any purpose other than the criminal proceedings in question (No. 18395/91, Dec. 7.12.92, not published).** 49. In the present case, the Commission has noted the following elements: first, there was no intrusion into the "inner circle" of the applicant's private life in the sense that the authorities entered his home and took the photographs there; secondly, the photographs related to a public incident, namely a manifestation of several persons in a public place, in which the applicant was voluntarily taking part; and thirdly, they were solely taken for the purposes, on 17 February 1988, of recording the character of the manifestation and the actual situation at the place in question, e.g. the sanitary conditions, and, on 19 February

1988, of recording the conduct of the participants in the manifestation in view of ensuing investigation proceedings for offences against the Road Traffic Regulations.

50. **In this context, the Commission attaches weight to the assurances given by the respondent Government according to which the individual persons on the photographs taken remained anonymous in that no names were noted down, the personal data recorded and photographs taken were not entered into a data processing system, and no action was taken to identify the persons photographed on that occasion by means of data processing.**

51. Bearing these factors in mind, the Commission finds that the taking of photographs of the applicant and their retention do not amount to an interference with his right to respect for his private life within the meaning of Article 8 para. 1 (Art. 8-1) of the Convention.

b. Establishment of the applicant's identity and recording of personal data

56. The Commission notes that S. 33 para. 1, in conjunction with S. 32 para. 1, of the Austrian Administrative Offences Act, authorizes the questioning of any person, suspected of having committed an administrative offence, to establish his identity. It considers that this provision also constitutes a sufficient legal basis for the subsequent retention of any information and material obtained.
Moreover, under the relevant provisions of the Road Traffic Regulations, both the obstruction of pedestrian traffic on pavements in built-up areas, as well as the unauthorised use of public roads for purposes other than traffic, constitute administrative offences.

57. **The Commission further observes that its power to review compliance with the relevant domestic legislation is limited under the Convention. It is in the first place for the national authorities, notably the courts, to interpret and to apply the domestic law (cf. Eur. Court H.R., Chorherr judgment of 25 August 1993, Series A no. 266-B, p. 36, para. 25). In the present case, the Austrian authorities had informed the participants in the manifestation about the unlawfulness of their activities under the Road Traffic Regulations. There is no indication that, at that time, the authorities did not act for the purpose of prosecuting the participants in this manifestation, though prosecution measures were not pursued against, among others, the applicant. The Commission notes that there was no finding of a domestic court on the question of lawfulness of the questioning and retention of the material obtained. Nevertheless, in the circumstances of the present case, there is no indication that the relevant provisions of the Austrian Administrative Offences Act and the Road Traffic Regulations were not observed.**

58. **The Commission is therefore satisfied that the interference was prescribed by Austrian law within the meaning of Article 8 para. 2 (Art. 8-2).**

64. **The Commission recalls that the Contracting States have a certain margin of appreciation in assessing the need for an interference, but it goes hand in hand with European supervision (Eur. Court H.R., Funke judgment of 23 February 1993, Series A no. 256-A, p. 24, para. 55).**

65. The Commission notes that officials of the police authorities

		questioned the applicant as to his identity on the occasion of his participation in a manifestation, considering that his conduct as well as the conduct of the other participants was unlawful under the relevant provisions of the Road Traffic Regulations. The Commission, proceeding from the basis that the authorities acted for the purposes of possibly bringing charges against the applicant and other participants in the manifestation, finds no element to show that this questioning went beyond what was necessary to establish the applicant's identity. 66. **As regards the retention of the information thus obtained in the administrative file on the manifestation, the Commission recalls that the keeping of records relating to criminal cases of the past can be regarded as necessary in a modern democratic society for the prevention of crime (cf. No. 1307/61, Dec. 4.10.62, Collection 9 p. 53), and that even if no criminal proceedings are subsequently brought and there is no reasonable suspicion against the individual concerned in relation to any specific offence, special considerations, such as combating organised terrorism, can justify the retention of the material concerned (McVeigh, O'Neill and Evans v. United Kingdom, Comm. Report, loc. cit., paras. 229-231). In the present case, the competent authorities established the applicant's and other participants' identity for the purposes of an ensuing prosecution for road traffic offences. This prosecution was not pursued in view of the trivial nature of the offences. However, the information obtained was only kept in a general administrative file recording the events in question. Moreover, this information was not entered into a data processing system. For these reasons, taking into account the margin of appreciation afforded to the Contracting Parties in such matters, the Commission finds that the relatively slight interference with the applicant's right to respect for his private life can reasonably be considered as necessary in a democratic society for the prevention of disorder and crime (cf. para. 60).** 67. The Commission concludes unanimously that there has been no violation of Article 8 (Art. 8) of the Convention.
9.	Eur. Court HR, *Z. v. Finland* judgment of 25 February 1997, 22009/93: disclosure of personal data; confidentiality of health data; appropriate safeguards; proportionality	94. In determining whether the impugned measures were "necessary in a democratic society", the Court will consider whether, in the light of the case as a whole, the reasons adduced to justify them were relevant and sufficient and whether the measures were proportionate to the legitimate aims pursued. 95. **In this connection, the Court will take into account that the protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general.** **Without such protection, those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as may be necessary in order to receive appropriate treatment and, even, from seeking such assistance, thereby endangering their own health and, in the case of transmissible diseases, that of the community (see Recommendation no. R (89) 14 on "The ethical issues of HIV infection in the health care and social settings", adopted by the Committee of Ministers of the Council of Europe on 24 October 1989, in particular the general observations**

on confidentiality of medical data in paragraph 165 of the explanatory memorandum).
The domestic law must therefore afford appropriate safeguards to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees in Article 8 of the Convention (see, mutatis mutandis, Articles 3 2 (c), 5, 6 and 9 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series no.108, Strasbourg, 1981).

96. **The above considerations are especially valid as regards protection of the confidentiality of information about a person's HIV infection. The disclosure of such data may dramatically affect his or her private and family life, as well as social and employment situation, by exposing him or her to opprobrium and the risk of ostracism. For this reason it may also discourage persons from seeking diagnosis or treatment and thus undermine any preventive efforts by the community to contain the pandemic (see the above-mentioned explanatory memorandum to Recommendation no. R (89) 14, paragraphs 166-68). The interests in protecting the confidentiality of such information will therefore weigh heavily in the balance in determining whether the interference was proportionate to the legitimate aim pursued. Such interference cannot be compatible with Article 8 of the Convention unless it is justified by an overriding requirement in the public interest.**
In view of the highly intimate and sensitive nature of information concerning a person's HIV status, any State measures compelling communication or disclosure of such information without the consent of the patient call for the most careful scrutiny on the part of the Court, as do the safeguards designed to secure an effective protection (see, mutatis mutandis, the Dudgeon v. the United Kingdom judgment of 22 October 1981, Series A no. 45, p. 21, 52; and the Johansen v. Norway judgment of 7 August 1996, Reports of Judgments and Decisions 1996-III, pp. 1003-04, 64).

97. **At the same time, the Court accepts that the interests of a patient and the community as a whole in protecting the confidentiality of medical data may be outweighed by the interest in investigation and prosecution of crime and in the publicity of court proceedings (see, mutatis mutandis, Article 9 of the above-mentioned 1981 Data Protection Convention), where such interests are shown to be of even greater importance.**

98. **It must be borne in mind in the context of the investigative measures in issue that it is not for the Court to substitute its views for those of the national authorities as to the relevance of evidence used in the judicial proceedings (see, for instance, the above-mentioned Johansen judgment, pp. 1006-07, 73).**

99. **As to the issues regarding access by the public to personal data, the Court recognises that a margin of appreciation should be left to the competent national authorities in striking a fair balance between the interest of publicity of court proceedings, on the one hand, and the interests of a party or a third person in maintaining the confidentiality of such data, on the other hand. The scope of this margin will depend on such factors as the nature and seriousness of the interests at stake and the gravity of the interference (see, for instance, the Leander v.Sweden judgment of 26 March 1987, Series A no.116, p. 25, 58; and, mutatis mutandis, the Manoussakis and Others v. Greece judgment of 26September 1996, Reports 1996-IV, 44).**

100. It is in the light of the above considerations that the Court will examine the contested interferences with the applicant's right to respect for her private and family life. Since the various measures were different in character, pursued distinct aims and infringed upon her private and family life to a different extent, the Court will examine the necessity of each measure in turn.

101. Before broaching these issues, the Court observes at the outset that, although the applicant may not have had an opportunity to be heard directly by the competent authorities before they took the measures, they had been made aware of her views and interests in these matters.
All her medical advisers had objected to the various orders to testify and had thus actively sought to protect her interests in maintaining the confidentiality of her medical data. At an early stage, her letter to senior doctor L., urging him not to testify and stating her reasons, had been read out to the City Court (see paragraphs 23, 26, 29 and 30 above).
In the above-mentioned letter, it was implicit, to say the least, that she would for the same reasons object also to the communication of her medical data by means of seizure of her medical records and their inclusion in the investigation file, which occurred a few days later (see paragraphs 31 and 32 above). According to the applicant, her lawyer had done all he could to draw the public prosecutor's attention to her objections to her medical data being used in the proceedings.
Moreover, before upholding the ten-year limitation on the confidentiality order, the Court of Appeal had been informed by X's lawyer of the applicant's wish that the period of confidentiality be extended (see paragraph 35 above).
In these circumstances, the Court is satisfied that the decision-making process leading to the measures in question was such as to take her views sufficiently into account for the purposes of Article 8 of the Convention (see, mutatis mutandis, the W. v. the United Kingdom judgment of 8 July 1987, Series A no. 121, pp. 28-29, 62-64; and the above-mentioned Johansen judgment, pp. 1004-05,§66). Thus, the procedure followed did not as such give rise to any breach of that Article.
In this connection, the Court takes note of the fact that, according to the Government's submissions to the Court, it would have been possible for the applicant to challenge the seizure before the City Court (see paragraph49 above). Also, as is apparent from the Supreme Court's decision of 1 September 1995, she was able under Finnish law to apply - by way of an extraordinary procedure - for an order quashing the Court of Appeal's judgment in so far as it permitted the information and material about her to be made accessible to the public as from 2002 (see paragraph 40 above).

(i) The orders requiring the applicant's doctors and psychiatrist to give evidence

102. As regards the orders requiring the applicant's doctors and psychiatrist to give evidence, the Court notes that the measures were taken in the context of Z availing herself of her right under Finnish law not to give evidence against her husband (see paragraphs 14, 17 and21 above). The object was exclusively to ascertain from her medical advisers when X had become aware of or had reason to suspect his HIV infection. Their evidence had the possibility of being at the material time decisive for the question whether X was guilty of sexual offences only or in addition of the more serious offence of attempted manslaughter in relation to two offences committed prior to 19March 1992, when the positive results of the HIV test had become available. There can be no doubt that the competent national authorities were entitled to think that

very weighty public interests militated in favour of the investigation and prosecution of X for attempted manslaughter in respect of all of the five offences concerned and not just three of them.

103. The Court further notes that, under the relevant Finnish law, the applicant's medical advisers could be ordered to give evidence concerning her without her informed consent only in very limited circumstances, namely in connection with the investigation and the bringing of charges for serious criminal offences for which at least six years' imprisonment was prescribed (see paragraph 46 above). Since they had refused to give evidence to the police, the latter had to obtain authorisation from a judicial body - the City Court - to hear them as witnesses (see paragraph 28 above). The questioning took place in camera before the City Court, which had ordered in advance that its file, including transcripts of witness statements, be kept confidential (see paragraphs 19 and 23 above). All those involved in the proceedings were under a duty to treat the information as confidential. Breach of their duty in this respect could lead to civil and/or criminal liability under Finnish law (see paragraphs 53-56 above).
The interference with the applicant's private and family life which the contested orders entailed was thus subjected to important limitations and was accompanied by effective and adequate safeguards against abuse (see, for instance, the Klass and Others v. Germany judgment of 6September 1978, Series A no. 28, pp. 23-24, 49-50; and the Leander judgment cited above, p. 25, 60).
In this connection, the Court sees no reason to question the extent to which the applicant's doctors were ordered to give evidence (see paragraphs 23, 26 and 30 above). As indicated above, the expediency of obtaining evidence is primarily a matter for the national authorities and it is not for the Court to substitute its views for theirs in this regard (see paragraph 98 above).

104. In view of the above factors, in particular the confidential nature of the proceedings against X, as well as their highly exceptional character, the Court is not persuaded by the applicant's argument that the various orders to give evidence were likely to have deterred potential and actual HIV carriers in Finland from undergoing blood tests and from seeking medical treatment.

105. In the light of the foregoing, **the Court finds that the various orders requiring the applicant's medical advisers to give evidence were supported by relevant and sufficient reasons which corresponded to an overriding requirement in the interest of the legitimate aims pursued. It is also satisfied that there was a reasonable relationship of proportionality between those measures and aims. Accordingly, there has been no violation of Article 8 on this point.**

(ii) Seizure of the applicant's medical records and their inclusion in the investigation file

106. The seizure of the applicant's medical records and their inclusion in the investigation file were complementary to the orders compelling the medical advisers to give evidence. Like the latter measures, the former were taken in the context of the applicant refusing to give evidence against her husband and their object was to ascertain when X had become aware of his HIV infection or had reason to suspect that he was carrying the disease. They were based on the same weighty public interests (see paragraph 102 above).

107. Furthermore, they were subject to similar limitations and safeguards

against abuse (see paragraph 103 above). The substantive conditions on which the material in question could be seized were equally restrictive (see paragraphs 46 and 48 above). More importantly, the material had been submitted in the context of proceedings held in camera, and the City Court had decided that the case documents should be treated as confidential, which measure was protected largely by the same rules and remedies as the witness statements (see paragraphs 23 and 53-56 above).

108. It is true, however, that the seizure, unlike the taking of evidence from the doctors and psychiatrist, had not been authorised by a court but had been ordered by the prosecution (see paragraph 31 above).
Nevertheless, under the terms of the relevant provision in chapter 4, section 2 (2), of the Coercive Means of Criminal Investigation Act, a condition for the seizure of the medical records concerned was that the applicant's doctors would be "entitled or obliged to give evidence in the pre-trial investigation about the matter contained in the document[s]"(see paragraph 48 above). The legal conditions for the seizure were thus essentially the same as those for the orders on the doctors to give evidence.
Furthermore, prior to the seizure of the documents, the City Court had already decided that at least two of the doctors should be heard, whilst it required all the other doctors to give evidence shortly afterwards (see paragraphs 23, 26 and 30 above). The day following the seizure, the City Court, which had power to exclude evidence, decided to include all the material in question in its case file (see paragraph 32 above). In addition, as already noted, the applicant had the possibility of challenging the seizure before the City Court (see paragraphs 49 and 101 above).
Therefore, the Court considers that the fact that the seizure was ordered by the prosecution and not by a court cannot of itself give rise to any misgivings under Article 8.

109. As to the applicant's submission that parts of the material had been irrelevant and that none of it had been decisive in the trial against X, the Court reiterates that the expediency of the adducing and admission of evidence by national authorities in domestic proceedings is primarily a matter to be assessed by them and that it is normally not within its province to substitute its views for theirs in this respect (see paragraph 98 above). Bearing in mind the arguments advanced by the Government as to the variety of data which could have been relevant for the determination of when X was first aware of or had reason to suspect his HIV infection (see paragraph 89 above), the Court sees no reason to doubt the assessment by the national authorities on this point.

110. Therefore, **the Court considers that the seizure of the applicant's medical records and their inclusion in the investigation file were supported by relevant and sufficient reasons, the weight of which was such as to override the applicant's interest in the information in question not being communicated. It is satisfied that the measures were proportionate to the legitimate aims pursued and, accordingly, finds no violation of Article 8 on this point either.**

(iii) Duration of the order to maintain the medical data confidential

111. As regards the complaint that the medical data in issue would become accessible to the public as from 2002, the Court notes that the ten-year limitation on the confidentiality order did not correspond to the wishes or interests of the litigants in the proceedings, all of whom had requested a longer period of confidentiality (see paragraph35 above).

112. The Court is not persuaded that, by prescribing a period of ten years,

		the domestic courts attached sufficient weight to the applicant's interests. It must be remembered that, as a result of the information in issue having been produced in the proceedings without her consent, she had already been subjected to a serious interference with her right to respect for private and family life. The further interference which she would suffer if the medical information were to be made accessible to the public after ten years is not supported by reasons which could be considered sufficient to override her interest in the data remaining confidential for a longer period. The order to make the material so accessible as early as 2002 would, if implemented, amount to a disproportionate interference with her right to respect for her private and family life, in violation of Article 8. However, the Court will confine itself to the above conclusion, as it is for the State to choose the means to be used in its domestic legal system for discharging its obligations under Article 53 of the Convention (see the Marckx v. Belgium judgment of 13 June 1979, Series A no. 31, pp. 25-26, 58). <u>(iv) Publication of the applicant's identity and health condition in the Court of Appeal's judgment</u> 113. Finally, the Court must examine whether there were sufficient reasons to justify the disclosure of the applicant's identity and HIV infection in the text of the Court of Appeal's judgment made available to the press (see paragraphs 36 and 43 above). Under the relevant Finnish law, the Court of Appeal had the discretion, firstly, to omit mentioning any names in the judgment permitting the identification of the applicant and, secondly, to keep the full reasoning confidential for a certain period and instead publish an abridged version of the reasoning, the operative part and an indication of the law which it had applied (see paragraph 52 above). In fact, it was along these lines that the City Court had published its judgment, without it giving rise to any adverse comment (see paragraph33 above). Irrespective of whether the applicant had expressly requested the Court of Appeal to omit disclosing her identity and medical condition, that court was informed by X's lawyer about her wishes that the confidentiality order be extended beyond ten years (see paragraph35 above). It evidently followed from this that she would be opposed to the disclosure of the information in question to the public. In these circumstances, and having regard to the considerations mentioned in paragraph 112 above, the Court does not find that the impugned publication was supported by any cogent reasons. Accordingly, the publication of the information concerned gave rise to a violation of the applicant's right to respect for her private and family life as guaranteed by Article 8. <u>(v) Recapitulation</u> 114. **The Court thus reaches the conclusions that there has been no violation of Article 8 of the Convention (1) with respect to the orders requiring the applicant's medical advisers to give evidence or (2) with regard to the seizure of her medical records and their inclusion in the investigation file.** **On the other hand, it finds (3) that making the medical data concerned accessible to the public as early as 2002 would, if implemented, give rise to a violation of this Article and (4) that there has been a violation thereof with regard to the publication of the applicant's identity and medical condition in the Court of Appeal's judgment.**
10	Eur. Court HR, *Halford*	44. **In the Court's view, it is clear from its case-law that telephone**

	v. The United Kingdom judgment of 25 June 1997, 20605/92: interception of communications; telephone tapping; secret surveillance; adequate protection against interferences	**calls made from business premises as well as from the home may be covered by the notions of "private life" and "correspondence" within the meaning of Article 8 (1) (see the above-mentioned Klass and Others judgment, loc. cit., the Malone v. the United Kingdom judgment of 2 August 1985, Series A no. 82, p. 30, (64), the above-mentioned Huvig judgment, loc. cit., and mutatis mutandis the above-mentioned Niemietz judgment, pp. 33-35, (29)-(33)).** 45. There is no evidence of any warning having been given to Ms Halford, as a user of the internal telecommunications system operated at the Merseyside Police Headquarters, that calls made on that system would be liable to interception. She would, the Court considers, have had a reasonable expectation of privacy for such calls, which expectation was moreover reinforced by a number of factors. As Assistant Chief Constable she had sole use of her office where there were two telephones, one of which was specifically designated for her private use. Furthermore, she had been given the assurance, in response to a memorandum, that she could use her office telephones for the purposes of her sex discrimination case (see paragraph 16 above). 46. For all of the above reasons, the Court concludes that telephone conversations made by Ms Halford on her office telephones fell within the scope of the notions of "private life" and "correspondence" and that Article 8 was therefore applicable to this part of the complaint. 49. **Article 8 (2) further provides that any interference by a public authority with an individual's right to respect for private life and correspondence must be "in accordance with the law". According to the Court's well-established case-law, this expression does not only necessitate compliance with domestic law, but also relates to the quality of that law, requiring it to be compatible with the rule of law. In the context of secret measures of surveillance or interception of communications by public authorities, because of the lack of public scrutiny and the risk of misuse of power, the domestic law must provide some protection to the individual against arbitrary interference with Article 8 rights. Thus, the domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in and conditions on which public authorities are empowered to resort to any such secret measures (see the above-mentioned Malone judgment, p. 32, (67), and, mutatis mutandis, the Leander v. Sweden judgment of 26 March 1987, Series A no. 116, p. 23, (50)-(51)).** 50. In the present case, the Government accepted that if, contrary to their submission, the Court were to conclude that there had been an interference with the applicant's rights under Article 8 in relation to her office telephones, such interference was not "in accordance with the law" since domestic law did not provide any regulation of interceptions of calls made on telecommunications systems outside the public network. 51. The Court notes that the 1985 Act does not apply to internal communications systems operated by public authorities, such as that at Merseyside Police Headquarters, and that there is no other provision in domestic law to regulate interceptions of telephone calls made on such systems (see paragraphs 36-37 above). **It cannot therefore be said that the interference was "in accordance with the law" for the purposes of Article 8 (2) of the Convention, since the domestic law did not provide adequate protection to Ms Halford against interferences by the police with her right to respect for her private life and correspondence.**

		It follows that there has been a violation of Article 8 in relation to the interception of calls made on Ms Halford's office telephones.
11.	Eur. Court HR, *M.S. v. Sweden* judgment of 27 August 1997, 20837/92: disclosure of personal data; medical records; health data; proportionality	35. The Court notes that the medical records in question contained highly personal and sensitive data about the applicant, including information relating to an abortion. Although the records remained confidential, they had been disclosed to another public authority and therefore to a wider circle of public servants (see paragraphs 12-13 above). Moreover, whilst the information had been collected and stored at the clinic in connection with medical treatment, its subsequent communication had served a different purpose, namely to enable the Office to examine her compensation claim. It did not follow from the fact that she had sought treatment at the clinic that she would consent to the data being disclosed to the Office (see paragraph 10 above). Having regard to these considerations, the Court finds that the disclosure of the data by the clinic to the Office entailed an interference with the applicant's right to respect for private life guaranteed by paragraph 1 of Article 8. It remains to be determined whether the interference was justified under paragraph 2 of Article 8. 41. **The Court reiterates that the protection of personal data, particularly medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general. The domestic law must afford appropriate safeguards to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees in Article 8 of the Convention (see the Z v. Finland judgment of 25 February 1997, Reports of Judgments and Decisions 1997-..., p. 2758, (95)).** **Bearing in mind the above considerations and the margin of appreciation enjoyed by the State in this area, the Court will examine whether, in the light of the case as a whole, the reasons adduced to justify the interference were relevant and sufficient and whether the measure was proportionate to the legitimate aim pursued (ibid., (94)).** 42. Turning to the particular circumstances, the Court notes that the applicant's medical data were communicated by one public institution to another in the context of an assessment of whether she satisfied the legal conditions for obtaining a benefit which she herself had requested (see paragraphs 11-14 above). It recognises that, in deciding whether to accept the applicant's compensation claim, the Office had a legitimate need to check information received from her against data in the possession of the clinic. In the absence of objective information from an independent source, it would have been difficult for the Office to determine whether the claim was well-founded. That claim concerned a back injury which she had allegedly suffered in 1981 and all the medical records produced by the clinic to the Office, including those concerning her abortion in 1985 and the treatment thereafter, contained information relevant to the applicant's back problems. As appears from the records of 1985, her back pains constituted the main reason for the termination of pregnancy (see paragraphs 12-13 above). Moreover, the data covered the period in respect of which she claimed compensation under the Insurance Act (see paragraphs 10-11 above). In the Court's view, the applicant has not substantiated her allegation that the clinic could not reasonably have considered her post

		1981 medical records to be material to the Office's decision. 43. In addition, under the relevant law it is a condition for imparting the data concerned that the Office has made a request and that the information be of importance for its application of the Insurance Act (see paragraph 18 above). Staff of the clinic could incur civil and/or criminal liability had they failed to observe these conditions (see paragraph 22 above). The Office, as the receiver of the information, was under a similar duty to treat the data as confidential, subject to similar rules and safeguards as the clinic (see paragraphs 20 and 22 above). **In the circumstances the contested measure was therefore subject to important limitations and was accompanied by effective and adequate safeguards against abuse (see the above-mentioned Z v. Finland judgment, (103)).** 44. Having regard to the foregoing, **the Court considers that there were relevant and sufficient reasons for the communication of the applicant's medical records by the clinic to the Office and that the measure was not disproportionate to the legitimate aim pursued. Accordingly, it concludes that there has been no violation of the applicant's right to respect for private life, as guaranteed by Article 8 of the Convention.**
12.	Eur. Court HR, *Kopp v. Switzerland* judgment of 25 March 1998, 23224/94: interception of communications, phone tapping; secret surveillance; protection against arbitrary interference	64. **The Court reiterates in that connection that Article 8 (2) requires the law in question to be "compatible with the rule of law". In the context of secret measures of surveillance or interception of communications by public authorities, because of the lack of public scrutiny and the risk of misuse of power, the domestic law must provide some protection to the individual against arbitrary interference with Article 8 rights. Thus, the domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in and conditions on which public authorities are empowered to resort to any such secret measures (see, as the most recent authority, the above-mentioned Halford judgment, p. 1017, (49)).** 73. However, the Court discerns a contradiction between the clear text of legislation which protects legal professional privilege when a lawyer is being monitored as a third party and the practice followed in the present case. Even though the case-law has established the principle, which is moreover generally accepted, that legal professional privilege covers only the relationship between a lawyer and his clients, the law does not clearly state how, under what conditions and by whom the distinction is to be drawn between matters specifically connected with a lawyer's work under instructions from a party to proceedings and those relating to activity other than that of counsel. 74. Above all, in practice, it is, to say the least, astonishing that this task should be assigned to an official of the Post Office's legal department, who is a member of the executive, without supervision by an independent judge, especially in this sensitive area of the confidential relations between a lawyer and his clients, which directly concern the rights of the defence. 75. **In short, Swiss law, whether written or unwritten, does not indicate with sufficient clarity the scope and manner of exercise of the authorities' discretion in the matter. Consequently, Mr Kopp, as a lawyer, did not enjoy the minimum degree of protection required by the rule of law in a democratic society. There has therefore been a breach of Article 8.**

13.	Eur. Court HR, *Lambert v. France* judgment of 24 August 1998, 23618/94: telephone tapping; preventing disorder; necessary in a democratic society; effective control	21. **The Court points out that as telephone conversations are covered by the notions of "private life" and "correspondence" within the meaning of Article 8, the admitted measure of interception amounted to "interference by a public authority" with the exercise of a right secured to the applicant in paragraph 1 of that Article (see, among other authorities, the following judgments: Malone v. the United Kingdom, 2 August 1984, Series A no. 82, p. 30, § 64; Kruslin v. France and Huvig v. France, 24 April 1990, Series A no. 176-A and B, p. 20, § 26, and p. 52, § 25; Halford v. the United Kingdom, 25 June 1997, Reports of Judgments and Decisions 1997-III, pp. 1016–17, § 48; and Kopp v. Switzerland, 25 March 1998, Reports 1998‑II, p. 540, § 53).** In this connection, it is of little importance that the telephone tapping in question was carried out on the line of a third party. The Government did not dispute this. 28. The Court considers, as the Commission did, that Articles 100 et seq. of the Code of Criminal Procedure, inserted by the Law of 10 July 1991 on the confidentiality of telecommunications messages, lay down clear, detailed rules and specify with sufficient clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities (see the Kruslin and Huvig judgments cited above, pp. 24–25, §§ 35–36, and p. 56, §§ 34–35, respectively, and, as the most recent authority and mutatis mutandis, the Kopp judgment cited above, pp. 541–43, §§ 62–75). 29. **The Court shares the opinion of the Government and the Commission and considers that the interference was designed to establish the truth in connection with criminal proceedings and therefore to prevent disorder.** 30. **It remains to be ascertained whether the interference was "necessary in a democratic society" for achieving those objectives. Under the Court's settled case-law, the Contracting States enjoy a certain margin of appreciation in assessing the existence and extent of such necessity, but this margin is subject to European supervision, embracing both the legislation and the decisions applying it, even those given by an independent court (see, mutatis mutandis, the Silver and Others v. the United Kingdom judgment of 25 March 1983, Series A no. 61, pp. 37–38, § 97, and the Barfod v. Denmark judgment of 22 February 1989, Series A no. 149, p. 12, § 28).** 31. **When considering the necessity of interference, the Court stated in its Klass and Others v. Germany judgment of 6 September 1978 (Series A no. 28, pp. 23 and 25–26, §§ 50, 54 and 55):** **"The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on ... [among other things] the kind of remedy provided by the national law.** **...** **It therefore has to be determined whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the 'interference' resulting from the contested legislation to what is 'necessary in a democratic society'.** **... In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded. One of the fundamental principles of a democratic society is the rule of law, which is expressly referred to in the Preamble to the Convention... The rule of law implies, inter alia, that an interference**

		by the executive authorities with an individual's rights should be subject to an effective control…" 40. **The Court therefore considers, like the Commission, that the applicant did not have available to him the "effective control" to which citizens are entitled under the rule of law and which would have been capable of restricting the interference in question to what was "necessary in a democratic society".** 41. There has consequently been a violation of Article 8 of the Convention.
14.	Eur. Court HR, *Valenzuela Contreras v. Spain*, judgment of 30 July 1998, 27671/95: interception of telephone conversations; secret surveillance; protection against arbitrary interference; requirement of foreseeability	46. **The following principles relevant in the instant case have been established by the Court in its case-law:** **(i) The interception of telephone conversations constitutes an interference by a public authority in the right to respect for private life and correspondence. Such an interference will be in breach of Article 8 § 2 unless it is "in accordance with the law", pursues one or more legitimate aims under paragraph 2 and, in addition, is "necessary in a democratic society" to achieve those aims (see the Kopp v. Switzerland judgment of 25 March 1998, Reports 1998- II, p. 539, § 50).** **(ii) The words "in accordance with the law" require firstly that the impugned measure should have some basis in domestic law. However, that expression does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law. The expression thus implies that there must be a measure of protection in domestic law against arbitrary interference by public authorities with the rights safeguarded by paragraph 1 (see the Malone judgment cited above, p. 32, § 67). From that requirement stems the need for the law to be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him (see the Kruslin judgment cited above p. 20, § 27, and the Kopp judgment cited above, p. 540, § 55).** **(iii) Especially where a power of the executive is exercised in secret the risks of arbitrariness are evident. In the context of secret measures of surveillance or interception by public authorities, the requirement of foreseeability implies that the domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in and conditions on which public authorities are empowered to take any such secret measures (see the Malone judgment cited above, pp. 31–32, §§ 66– 67, the Kruslin judgment cited above, pp. 22–23, § 30, the Halford v. the United Kingdom judgment of 25 June 1997, Reports 1997-III, p. 1017, § 49, and the Kopp judgment cited above, p. 541, § 64). It is essential to have clear, detailed rules on the subject, especially as the technology available for use is constantly becoming more sophisticated (see the Kruslin judgment cited above, p. 23, § 33, the Huvig judgment cited above, p. 55, § 32, and the Kopp judgment cited above, pp. 542–43, § 72).** **(iv) The Kruslin and Huvig judgments mention the following minimum safeguards that should be set out in the statute in order to avoid abuses of power: a definition of the categories of people liable to have their telephones tapped by judicial order, the nature of the offences which may give rise to such an order, a limit on the duration of telephone tapping, the procedure for drawing up the summary reports containing intercepted conversations, the precautions to be taken in order to communicate the recordings intact and in their entirety for possible inspection by the judge and by the defence and the circumstances in which recordings may or must be erased or the tapes destroyed, in particular where an accused has been discharged by an investigating judge or acquitted by a court (loc. cit. p. 24, § 35,**

and p. 56, § 34, respectively).

47. The tapping of Mr Valenzuela Contreras's telephone line between 26 November and 20 December 1985 (see paragraphs 14 and 16 above) constitutes an "interference by a public authority" within the meaning of Article 8 § 2 in the applicant's exercise of his right to respect for his private life and correspondence. Indeed, that point was not disputed. Nor is it decisive in that regard that, as the Government intimated, only a "metering" system was used (see the Malone judgment cited above, p. 38, § 87).

53. The Court must therefore assess the quality of the legal rules that were applied in Mr Valenzuela Contreras's case.

59. **The Court notes that some of the conditions necessary under the Convention to ensure the foreseeability of the effects of the "law" and, consequently, to guarantee respect for private life and correspondence are not included either in Article 18 § 3 of the Constitution or in the provisions of the Code of Criminal Procedure cited in the order of 19 November 1985 (see paragraphs 14 and 30 above). They include, in particular, the conditions regarding the definition of the categories of people liable to have their telephones tapped by judicial order, the nature of the offences which may give rise to such an order, a limit on the duration of telephone tapping, the procedure for drawing up the summary reports containing intercepted conversations and the use and destruction of the recordings made (see paragraph 46(iv) above).**

60. Like the Delegate of the Commission, the Court cannot accept the Government's argument that the judge who ordered the monitoring of the applicant's telephone conversations could not have been expected to know the conditions laid down in the Kruslin and Huvig judgments five years before those judgments were delivered in 1990. It reiterates that the conditions referred to in the judgment cited by the Government concerning the quality of the law stem from the Convention itself. The requirement that the effects of the "law" be foreseeable means, in the sphere of monitoring telephone communications, that the guarantees stating the extent of the authorities' discretion and the manner in which it is to be exercised must be set out in detail in domestic law so that it has a binding force which circumscribes the judges' discretion in the application of such measures (see paragraph 46(iii) and (iv) above). Consequently, the Spanish "law" which the investigating judge had to apply should have provided those guarantees
with sufficient precision. The Court further notes that at the time the order for the monitoring of the applicant's telephone line was made it had already stated, in a judgment in which it had found a violation of Article 8, that "the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence" (see the Malone judgment cited above, p. 32, § 67). In addition, it points out that in any event the investigating judge who ordered the monitoring of the applicant's telephone communications had himself put in place a number of guarantees which, as the Government said, did not become a requirement of the case-law until much later.

61. **In summary, Spanish law, both written and unwritten, did not indicate with sufficient clarity at the material time the extent of the authorities' discretion in the domain concerned or the way in which it should be exercised. Mr Valenzuela Contreras did not, therefore,**

		enjoy the minimum degree of legal protection to which citizens are entitled under the rule of law in a democratic society (see the Malone judgment cited above, p. 36, § 79). There has therefore been a violation of Article 8.
15.	Eur. Court HR, *Amann v. Switzerland* judgment of 16 February 2000, 27798/95: interception of communications; telephone tapping; secret surveillance; requirement of foreseeability; discretionary power	50. **The Court draws attention to its established case-law, according to which the expression "in accordance with the law" not only requires that the impugned measure should have some basis in domestic law, but also refers to the quality of the law in question, requiring that it should be accessible to the person concerned and foreseeable as to its effects (see the Kopp judgment cited above, p. 540, § 55).** 56. **According to the Court's established case-law, a rule is "foreseeable" if it is formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct (see the Malone v. the United Kingdom judgment of 2 August 1984, Series A no. 82, pp. 31-32, § 66). With regard to secret surveillance measures the Court has underlined the importance of that concept in the following terms (ibid., pp. 32-33, §§ 67-68): "The Court would reiterate its opinion that the phrase 'in accordance with the law' does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention ... The phrase thus implies – and this follows from the object and purpose of Article 8 – that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by paragraph 1 ... Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident...** **... Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference."** **It has also stated that "tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a 'law' that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated" (see the Kopp judgment cited above, pp. 542-43, § 72).** 57. The "quality" of the legal provisions relied on in the instant case must therefore be considered. 58. The Court points out first of all that Article 1 of the Federal Council's Decree of 29 April 1958 on the Police Service of the Federal Public Prosecutor's Office, according to which the federal police "shall provide an investigation and information service in the interests of the Confederation's internal and external security", including by means of "surveillance" measures, contains no indication as to the persons concerned by such measures, the circumstances in which they may be ordered, the means to be employed or the procedures to be observed. That rule cannot therefore be considered to be sufficiently clear and

detailed to afford appropriate protection against interference by the authorities with the applicant's right to respect for his private life and correspondence.

59. It considers that the same is true of section 17(3) FCPA, which is drafted in similar terms.

62. **The Court concludes that the interference cannot therefore be considered to have been "in accordance with the law" since Swiss law does not indicate with sufficient clarity the scope and conditions of exercise of the authorities' discretionary power in the area under consideration. It follows that there has been a violation of Article 8 of the Convention arising from the recording of the telephone call received by the applicant on 12 October 1981 from a person at the former Soviet embassy in Berne.**

65. **The Court reiterates that the storing of data relating to the "private life" of an individual falls within the application of Article 8 § 1 (see the Leander v. Sweden judgment of 26 March 1987, Series A no. 116, p. 22, § 48). It points out in this connection that the term "private life" must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings; furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life" (see the Niemietz v. Germany judgment of 16 December 1992, Series A no. 251-B, pp. 33-34, § 29, and the Halford judgment cited above, pp. 1015-16, § 42). That broad interpretation corresponds with that of the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985 and whose purpose is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such personal data being defined as "any information relating to an identified or identifiable individual" (Article 2).**

69. **The Court reiterates that the storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding (see, mutatis mutandis, the Leander judgment cited above, p. 22, § 48, and the Kopp judgment cited above, p. 540, § 53).**

70. In the instant case the Court notes that a card containing data relating to the applicant's private life was filled in by the Public Prosecutor's Office and stored in the Confederation's card index. In that connection it points out that it is not for the Court to speculate as to whether the information gathered on the applicant was sensitive or not or as to whether the applicant had been inconvenienced in any way. It is sufficient for it to find that data relating to the private life of an individual were stored by a public authority to conclude that, in the instant case, the creation and storing of the impugned card amounted to an interference, within the meaning of Article 8, with the applicant's right to respect for his private life.

75. The Court notes that in December 1981, when the card on the applicant was created, the Federal Criminal Procedure Act, the Federal Council's Decree of 29 April 1958 on the Police Service of the Federal

		Public Prosecutor's Office and the Federal Council's Directives of 16 March 1981 applicable to the Processing of Personal Data in the Federal Administration were in force. None of those provisions, however, expressly mentions the existence of a register kept by the Public Prosecutor's Office, which raises the question whether there was "a legal basis in Swiss law" for the creation of the card in question and, if so, whether that legal basis was "accessible" (see the Leander judgment cited above, p. 23, § 51). It observes in that connection that the Federal Council's Directives of 16 March 1981 were above all intended for the staff of the federal administration. In the instant case, however, it does not consider it necessary to rule on this subject, since even supposing that there was an accessible legal basis for the creation of the card in December 1981, that basis was not "foreseeable". 76. The Court has found above (see paragraphs 58 and 59) that section 17(3) FCPA and Article 1 of the Federal Council's Decree of 29 April 1958 on the Police Service of the Federal Public Prosecutor's Office were drafted in terms too general to satisfy the requirement of foreseeability in the field of telephone tapping. For the reasons already set out, it arrives at the same conclusion concerning the creation of the card on the applicant. As regards the Federal Council's Directives of 16 March 1981 applicable to the Processing of Personal Data in the Federal Administration, they set out some general principles, for example that "there must be a legal basis for the processing of personal data" (section 411) or that "personal data may be processed only for very specific purposes" (section 412), but do not contain any appropriate indication as to the scope and conditions of exercise of the power conferred on the Public Prosecutor's Office to gather, record and store information; thus, they do not specify the conditions in which cards may be created, the procedures that have to be followed, the information which may be stored or comments which might be forbidden. Those directives, like the Federal Criminal Procedure Act and the Federal Council's Decree of 29 April 1958 on the Police Service of the Federal Public Prosecutor's Office, cannot therefore be considered sufficiently clear and detailed to guarantee adequate protection against interference by the authorities with the applicant's right to respect for his private life. 80. **The Court concludes that both the creation of the impugned card by the Public Prosecutor's Office and the storing of it in the Confederation's card index amounted to interference with the applicant's private life which cannot be considered to be "in accordance with the law" since Swiss law does not indicate with sufficient clarity the scope and conditions of exercise of the authorities' discretionary power in the area under consideration. It follows that there has been a violation of Article 8 of the Convention.**
16.	Eur. Court HR, *Rotaru v. Romania* judgment of 4 May 2000, 28341/95: erasure or destruction of personal data; storage in secret registers; requirement of foreseeability; safeguards; discretionary power	43. **The Court reiterates that the storing of information relating to an individual's private life in a secret register and the release of such information come within the scope of Article 8 § 1 (see the Leander v. Sweden judgment of 26 March 1987, Series A no. 116, p. 22, § 48).** **Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings: furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life" (see the Niemietz v. Germany judgment of 16 December 1992, Series A no. 251-B, pp. 33-34, § 29, and the Halford v. the United Kingdom judgment of 25 June 1997, Reports 1997-III, pp. 1015-16, §§ 42-46).** **The Court has already emphasised the correspondence of this broad interpretation with that of the Council of Europe's Convention of 28**

January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985 and whose purpose is "to secure ... for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy with regard to automatic processing of personal data relating to him" (Article 1), such personal data being defined in Article 2 as "any information relating to an identified or identifiable individual" (see Amann v. Switzerland [GC], no. 27798/95, § 65, ECHR 2000-II).
Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past.

44. **In the instant case the Court notes that the RIS's letter of 19 December 1990 contained various pieces of information about the applicant's life, in particular his studies, his political activities and his criminal record, some of which had been gathered more than fifty years earlier. In the Court's opinion, such information, when systematically collected and stored in a file held by agents of the State, falls within the scope of "private life" for the purposes of Article 8 § 1 of the Convention. That is all the more so in the instant case as some of the information has been declared false and is likely to injure the applicant's reputation. Article 8 consequently applies.**

46. **The Court points out that both the storing by a public authority of information relating to an individual's private life and the use of it and the refusal to allow an opportunity for it to be refuted amount to interference with the right to respect for private life secured in Article 8 § 1 of the Convention (see the following judgments: Leander cited above, p. 22, § 48; Kopp v. Switzerland, 25 March 1998, Reports 1998-II, p. 540, § 53; and Amann cited above, §§ 69 and 80).**
In the instant case it is clear beyond peradventure from the RIS's letter of 19 December 1990 that the RIS held information about the applicant's private life. While that letter admittedly predates the Convention's entry into force in respect of Romania on 20 June 1994, the Government did not submit that the RIS had ceased to hold information about the applicant's private life after that date. The Court also notes that use was made of some of the information after that date, for example in connection with the application for review which led to the decision of 25 November 1997.
Both the storing of that information and the use of it, which were coupled with a refusal to allow the applicant an opportunity to refute it, amounted to interference with his right to respect for his private life as guaranteed by Article 8 § 1.

52. **The Court reiterates its settled case-law, according to which the expression "in accordance with the law" not only requires that the impugned measure should have some basis in domestic law, but also refers to the quality of the law in question, requiring that it should be accessible to the person concerned and foreseeable as to its effects (see, as the most recent authority, Amann cited above, § 50).**

55. **As regards the requirement of foreseeability, the Court reiterates that a rule is "foreseeable" if it is formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct. The Court has stressed the importance of this concept with regard to secret surveillance in the following terms (see the Malone v. the United Kingdom judgment of 2 August 1984, Series A no. 82, p. 32, § 67, reiterated in Amann cited above, § 56):**
"The Court would reiterate its opinion that the phrase 'in accordance

with the law' does not merely refer back to domestic law but also relates to the quality of the 'law', requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention ... The phrase thus implies – and this follows from the object and purpose of Article 8 – that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by paragraph 1 ... Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident ...
... Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference."

56. The "quality" of the legal rules relied on in this case must therefore be scrutinised, with a view, in particular, to ascertaining whether domestic law laid down with sufficient precision the circumstances in which the RIS could store and make use of information relating to the applicant's private life.

57. The Court notes in this connection that section 8 of Law no. 14/1992 provides that information affecting national security may be gathered, recorded and archived in secret files.
No provision of domestic law, however, lays down any limits on the exercise of those powers. Thus, for instance, the aforesaid Law does not define the kind of information that may be recorded, the categories of people against whom surveillance measures such as gathering and keeping information may be taken, the circumstances in which such measures may be taken or the procedure to be followed. Similarly, the Law does not lay down limits on the age of information held or the length of time for which it may be kept.
Section 45 of the Law empowers the RIS to take over for storage and use the archives that belonged to the former intelligence services operating on Romanian territory and allows inspection of RIS documents with the Director's consent.
The Court notes that this section contains no explicit, detailed provision concerning the persons authorised to consult the files, the nature of the files, the procedure to be followed or the use that may be made of the information thus obtained.

58. It also notes that although section 2 of the Law empowers the relevant authorities to permit interferences necessary to prevent and counteract threats to national security, the ground allowing such interferences is not laid down with sufficient precision.

59. **The Court must also be satisfied that there exist adequate and effective safeguards against abuse, since a system of secret surveillance designed to protect national security entails the risk of undermining or even destroying democracy on the ground of defending it (see the Klass and Others judgment cited above, pp. 23-24, §§ 49-50).**
In order for systems of secret surveillance to be compatible with Article 8 of the Convention, they must contain safeguards established by law which apply to the supervision of the relevant services'

		activities. Supervision procedures must follow the values of a democratic society as faithfully as possible, in particular the rule of law, which is expressly referred to in the Preamble to the Convention. The rule of law implies, inter alia, that interference by the executive authorities with an individual's rights should be subject to effective supervision, which should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure (see the Klass and Others judgment cited above, pp. 25-26, § 55). 60. **In the instant case the Court notes that the Romanian system for gathering and archiving information does not provide such safeguards, no supervision procedure being provided by Law no. 14/1992, whether while the measure ordered is in force or afterwards.** 61. **That being so, the Court considers that domestic law does not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities.** 62. The Court concludes that the holding and use by the RIS of information on the applicant's private life were not "in accordance with the law", a fact that suffices to constitute a violation of Article 8. Furthermore, in the instant case that fact prevents the Court from reviewing the legitimacy of the aim pursued by the measures ordered and determining whether they were – assuming the aim to have been legitimate – "necessary in a democratic society". 63. There has consequently been a violation of Article 8.
17.	Eur. Court HR *Khan v. the United Kingdom* judgment of 12 May 2000, 35394/97: secret surveillance; use of covert listening devices; quality of law	26. **The Court recalls, with the Commission in the Govell case (see paragraphs 61 and 62 of the report cited above), that the phrase "in accordance with the law" not only requires compliance with domestic law but also relates to the quality of that law, requiring it to be compatible with the rule of law (see the Halford v. the United Kingdom judgment of 25 June 1997, Reports of Judgments and Decisions 1997-III, p. 1017, § 49). In the context of covert surveillance by public authorities, in this instance the police, domestic law must provide protection against arbitrary interference with an individual's right under Article 8. Moreover, the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which public authorities are entitled to resort to such covert measures (see the Malone v. the United Kingdom judgment of 2 August 1984, Series A no. 82, p. 32, § 67).** 27. At the time of the events in the present case, there existed no statutory system to regulate the use of covert listening devices, although the Police Act 1997 now provides such a statutory framework. The Home Office Guidelines at the relevant time were neither legally binding nor were they directly publicly accessible. The Court also notes that Lord Nolan in the House of Lords commented that under English law there is, in general, nothing unlawful about a breach of privacy. There was, therefore, no domestic law regulating the use of covert listening devices at the relevant time. 28. It follows that the interference in the present case cannot be considered to be "in accordance with the law", as required by Article 8 § 2 of the Convention. Accordingly, there has been a violation of Article 8.

18.	Eur. Court HR, *P.G. and J.H. v. the United Kingdom* judgment of 25 September 2001, 44787/98: secret surveillance; voice samples; covert listening devices; in accordance with the law	37. **The Court notes that it is not disputed that the surveillance carried out by the police at B.'s flat amounted to an interference with the right of the applicants to respect for their private life. As regards conformity with the requirements of the second paragraph of Article 8 – that any such interference be "in accordance with the law" and "necessary in a democratic society" for one or more of the specified aims – it is conceded by the Government that the interference was not "in accordance with the law" as at the time of the events there existed no statutory system to regulate the use of covert listening devices. Such measures were governed by the Home Office Guidelines, which were neither legally binding nor directly publicly accessible.** 38. **As there was no domestic law regulating the use of covert listening devices at the relevant time (see Khan, cited above, §§ 26-28), the interference in this case was not "in accordance with the law" as required by Article 8 § 2 of the Convention, and there has therefore been a violation of Article 8 in this regard. In the light of this conclusion, the Court is not required to determine whether the interference was, at the same time, "necessary in a democratic society" for one of the aims enumerated in paragraph 2 of Article 8.** <u>B. Concerning information obtained about the use of B.'s telephone</u> 42. **It is not in dispute that the obtaining by the police of information relating to the numbers called on the telephone in B.'s flat interfered with the private lives or correspondence (in the sense of telephone communications) of the applicants who made use of the telephone in the flat or were telephoned from the flat. The Court notes, however, that metering, which does not per se offend against Article 8 if, for example, done by the telephone company for billing purposes, is by its very nature to be distinguished from the interception of communications which may be undesirable and illegitimate in a democratic society unless justified (see Malone, cited above, pp. 37-38, §§ 83-84).** 46. **The Court observes that the quality of law criterion in this context refers essentially to considerations of foreseeability and lack of arbitrariness (see Kopp, cited above, p. 541, § 64). What is required by way of safeguard will depend, to some extent at least, on the nature and extent of the interference in question. In this case, the information obtained concerned the telephone numbers called from B.'s flat between two specific dates. It did not include any information about the contents of those calls, or who made or received them. The data obtained, and the use that could be made of them, were therefore strictly limited.** 47. While it does not appear that there are any specific statutory provisions (as opposed to internal policy guidelines) governing storage and destruction of such information, the Court is not persuaded that the lack of such detailed formal regulation raises any risk of arbitrariness or misuse. Nor is it apparent that there was any lack of foreseeability. Disclosure to the police was permitted under the relevant statutory framework where necessary for the purposes of the detection and prevention of crime, and the material was used at the applicants' trial on criminal charges to corroborate other evidence relevant to the timing of telephone calls. It is not apparent that the applicants did not have an adequate indication as to the circumstances in, and conditions on, which the public authorities were empowered to resort to such a measure.

48. **The Court concludes that the measure in question was "in accordance with the law".**

C. Concerning the use of listening devices in the police station

(a) The existence of an interference with private life

56. **Private life is a broad term not susceptible to exhaustive definition. The Court has already held that elements such as gender identification, name and sexual orientation and sexual life are important elements of the personal sphere protected by Article 8 (see, for example, B. v. France, judgment of 25 March 1992, Series A no. 232-C, pp. 53-54, § 63; Burghartz v. Switzerland, judgment of 22 February 1994, Series A no. 280-B, p. 28, § 24; Dudgeon v. the United Kingdom, judgment of 22 October 1981, Series A no. 45, pp. 18-19, § 41; and Laskey, Jaggard and Brown v. the United Kingdom, judgment of 19 February 1997, Reports 1997-1, p. 131, § 36). Article 8 also protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world (see, for example, Burghartz, cited above, opinion of the Commission, p. 37, § 47, and Friedl v. Austria, judgment of 31 January 1995, Series A no. 305-B, opinion of the Commission, p. 20, § 45). It may include activities of a professional or business nature (see Niemietz v. Germany, judgment of 16 December 1992, Series A no. 251-B, pp. 33-34, § 29, and Halford, cited above, p. 1016, § 44). There is therefore a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life".**

57. **There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method (see Rotaru v. Romania [GC], no. 28341/95, §§ 43-44, ECHR 2000-V). The Court has referred in this context to the Council of Europe's Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data, which came into force on 1 October 1985 and whose purpose is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such data being defined as "any information relating to an identified or identifiable individual" (Article 2) (see Amann v. Switzerland [GC], no. 27798/95, §§ 65-67, ECHR 2000-II, where the storing of information about the applicant on a card in a file was found to be an interference with private life, even though it contained no sensitive information and had probably never been consulted).**

58. In the case of photographs, the Commission previously had regard, for the purpose of delimiting the scope of protection afforded by Article 8 against arbitrary interference by public authorities, to whether the taking of the photographs amounted to an intrusion into the individual's privacy, whether the photographs related to private matters or public incidents and whether the material obtained was envisaged for a limited use or was likely to be made available to the general public (see Friedl, cited above, opinion of the Commission, p. 21, §§ 49-52). Where photographs were taken of an applicant at a public demonstration in a public place and retained by the police in a file, the Commission found no interference with private life, giving weight to the fact that the photograph was taken and retained as a record of the demonstration and no action had been taken to identify the persons photographed on that occasion by means of data processing (ibid., §§ 51-52).

59. **The Court's case-law has, on numerous occasions, found that the covert taping of telephone conversations falls within the scope of Article 8 in both aspects of the right guaranteed, namely, respect for private life and correspondence. While it is generally the case that the recordings were made for the purpose of using the content of the conversations in some way, the Court is not persuaded that recordings taken for use as voice samples can be regarded as falling outside the scope of the protection afforded by Article 8. A permanent record has nonetheless been made of the person's voice and it is subject to a process of analysis directly relevant to identifying that person in the context of other personal data. Though it is true that when being charged the applicants answered formal questions in a place where police officers were listening to them, the recording and analysis of their voices on this occasion must still be regarded as concerning the processing of personal data about the applicants.**

60. **The Court concludes therefore that the recording of the applicants' voices when being charged and when in their police cell discloses an interference with their right to respect for private life within the meaning of Article 8 § 1 of the Convention.**

(b) Compliance with the requirements of the second paragraph of Article 8

61. The Court has examined, firstly, whether the interference was "in accordance with the law." As noted above, this criterion comprises two main requirements: that there be some basis in domestic law for the measure and that the **quality of the law** is such as to **provide safeguards against arbitrariness** (see paragraph 44).

62. **It recalls that the Government relied as the legal basis for the measure on the general powers of the police to store and gather evidence. While it may be permissible to rely on the implied powers of police officers to note evidence and collect and store exhibits for steps taken in the course of an investigation, it is trite law that specific statutory or other express legal authority is required for more invasive measures, whether searching private property or taking personal body samples. The Court has found that the lack of any express basis in law for the interception of telephone calls on public and private telephone systems and for using covert surveillance devices on private premises does not conform with the requirement of lawfulness (see Malone, Halford and Khan, all cited above). It considers that no material difference arises where the recording device is operated, without the knowledge or consent of**

		the individual concerned, on police premises. The underlying principle that domestic law should provide protection against arbitrariness and abuse in the use of covert surveillance techniques applies equally in that situation. 63. The Court notes that the Regulation of Investigatory Powers Act 2000 contains provisions concerning covert surveillance on police premises. However, **at the relevant time, there existed no statutory system to regulate the use of covert listening devices by the police on their own premises. The interference was not therefore "in accordance with the law" as required by the second paragraph of Article 8 and there has been a violation of this provision.** In these circumstances, an examination of the necessity of the interference is no longer required.
19.	Eur. Court HR, *Armstrong v. the United Kingdom* judgment of 16 July 2002, 48521/99: covert recording devices; secret surveillance	20. The Court recalls, as in the above-mentioned Khan case, that at the relevant time there existed no statutory system to regulate the use of covert recording devices by the police. The interferences disclosed by the measures implemented in respect of the applicant were therefore not "in accordance with the law" as required by the second paragraph of Article 8 and there has accordingly been a violation of this provision.
20	Eur. Court HR, *Taylor-Sabori v. the United Kingdom* judgment of 22 October 2002, 47114/99: secret surveillance; quality of the law; interception of pager messages	18. **The Court notes that it is not disputed that the surveillance carried out by the police in the present case amounted to an interference with the applicant's rights under Article 8 § 1 of the Convention. It recalls that the phrase "in accordance with the law" not only requires compliance with domestic law but also relates to the quality of that law, requiring it to be compatible with the rule of law. In the context of covert surveillance by public authorities, in this instance the police, domestic law must provide protection against arbitrary interference with an individual's right under Article 8. Moreover, the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which public authorities are entitled to resort to such covert measures (see Khan v. the United Kingdom, no. 35394/97, § 26, ECHR 2000-V).** 19. At the time of the events in the present case there existed no statutory system to regulate the interception of pager messages transmitted via a private telecommunication system. It follows, as indeed the Government have accepted, that the interference was not "in accordance with the law". There has, accordingly, been a violation of Article 8.
21.	Eur. Court HR, *Allan v. the United Kingdom* judgment of 5 November 2002, 48539/99: audio and video recording devices; secret surveillance	35. The Government accepted, following the judgment in Khan v. the United Kingdom (no. 35394/97, [Section 3], ECHR 2000-V, judgment of 12 May 2000, §§ 26-28) that the use of the audio and video recording devices in the applicant's cell, the prison visiting area and on a fellow prisoner amounted to an interference with the applicant's right to private life under Article 8 § 1 of the Convention and that the measures were not used "in accordance with law" within the meaning of Article 8 § 2 of the Convention. 36. **The Court recalls, as in the above-mentioned Khan case, that at the relevant time there existed no statutory system to regulate the use of covert recording devices by the police. The interferences disclosed by the measures implemented in respect of the applicant were therefore not "in accordance with the law" as required by the second paragraph of Article 8 and there have thus been violations of this provision.**

22.	Eur. Court HR, *Cotlet v. Romania* judgment of 3 June 2003, 38565/97: intereception of correspondence; positive obligations	**Judgment in French** From the Information Note No. 54: Facts: The applicant, who is serving a prison sentence for murder, lodged an application with the European Commission of Human Rights in 1995. He stated that the letters sent by the Commission had been opened when they reached him and that he was required to hand his letters to the Commission to the prison authorities in an unsealed envelope; subsequently, a letter from the Registry of the European Court of Human Rights reached him in an envelope which had been opened. His correspondence with the Commission and then with the Court was delayed. In March 1999, the applicant complained that he had been prevented from writing to the Court because the authorities refused to supply him with writing paper and envelopes. The applicant further stated that his correspondence with the Convention organs had attracted the hostility of the prison administration and expressed his fears on that subject. Law: Article 8 - The refusal of the prison administration to supply the applicant with the envelopes, stamps and writing paper necessary for his correspondence with the Court constitutes a failure by the respondent State to comply with its positive obligation to ensure effective observance of the applicantís right to respect for his correspondence. Conclusion: violation (unanimously). The Court concludes that there has been a violation of Article 8 owing to the delays in forwarding his letters to the Commission and the opening of the letters to or from the Commission and the Court (cf. the Petra v. Romania judgment of 23 September 1998). Discussion of violation in §§ 30-65 30. La Cour relève que ce grief comporte trois branches: la première a trait aux délais d'acheminement du courrier du requérant destiné à la Commission ou à la Cour ; la deuxième concerne l'ouverture du courrier du requérant destiné à la Commission et à la Cour ou émanant de celles-ci ; la troisième porte sur le refus de l'administration du pénitencier de fournir au requérant le nécessaire pour sa correspondance avec la Cour. 1 Sur le délai d'acheminement du courrier du requérant destiné à la Commission et à la Cour B. Appréciation de la Cour 33. La Cour note d'emblée que cette branche du grief du requérant porte sur la période allant du 16 novembre 1995, date à laquelle le requérant a envoyé une première lettre à la Commission, au 20 octobre 1997, date à laquelle est parvenue à cette dernière la lettre du requérant du 22 août 1997. Elle relève que, pendant cette période, le courrier du requérant est parvenu à destination dans des délais compris entre un mois et dix jours minimum et deux mois et six jours maximum. La Cour relève qu'après le 20 octobre 1997, les lettres du requérant lui parvinrent dans des délais normaux, généralement de une à deux semaines après leur envoi (paragraphe 22 ci-dessus). Partant, elle estime, sur la base des éléments fournis, qu'aucune ingérence ne saurait être décelée après le 20 octobre 1997 en raisons du délai d'acheminement du courrier du requérant destiné à la Cour. 34. La Cour note ensuite qu'il n'est pas contesté que le retard dans l'acheminement du courrier du requérant entre les 16 novembre 1995 et 20 octobre 1997 constitue, en l'occurrence, une ingérence au droit au respect de sa correspondance, garanti par l'article 8 § 1 de la Convention,

qui n'était pas prévue par une « loi », au sens du paragraphe 2 de l'article 8 de la Convention.

35. A cet égard, la Cour rappelle que, dans l'affaire Petra précitée, elle a conclu à la violation de l'article 8 de la Convention au motif que « la loi roumaine n'indiquait pas avec assez de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités » (Petra, précité, § 38 in fine), et que « les dispositions internes applicables en matière de contrôle de la correspondance des détenus (...) laissent aux autorités nationales une trop grande latitude : ils se limitent notamment à indiquer, de façon très générale, le droit des condamnés de recevoir et d'envoyer du courrier et accordent aux directeurs des établissements pénitentiaires le pouvoir de garder toute lettre ou tout journal, livre ou magazine non appropriés à la rééducation du condamné. Le contrôle de la correspondance semble donc être automatique, indépendant de toute décision d'une autorité judiciaire et non assujetti à des voies de recours. Quant au règlement d'application, il n'est pas publié, de sorte que le requérant n'a pas pu en prendre connaissance » (Petra, précité, § 37).

36. La Cour estime que rien en l'espèce ne permet de distinguer de ce point de vue la présente affaire de l'affaire Petra précitée. L'ingérence litigieuse étant fondée en l'occurrence sur les mêmes dispositions internes que celles déjà jugées comme étant incompatibles avec les exigences d'une « loi », au sens de l'article 8 § 2 de la Convention, la Cour conclut donc qu'elle n'était pas prévue par la « loi » et que, partant, il y a eu, sur ce point, une violation de l'article 8 de la Convention.

37. Eu égard à la conclusion qui précède, la Cour n'estime pas nécessaire de vérifier en l'espèce le respect des autres exigences du paragraphe 2 de l'article 8, ni la qualité de « loi », au sens du paragraphe 2 précité, de l'arrêté du ministre de la Justice du 24 novembre 1997 auquel renvoie le Gouvernement, car postérieur aux faits constitutifs de cette branche du grief tiré de l'article 8 de la Convention.

2. Sur l'ouverture du courrier du requérant destiné à la Commission et à la Cour ou émanant de celles-ci

B. Appréciation de la Cour

1. Période allant jusqu'au 24 novembre 1997

40. La Cour relève qu'il n'est pas contesté en l'espèce que l'ouverture du courrier du requérant destiné à la Commission ou émanant de celle-ci avant le 24 novembre 1997 constitue, en l'occurrence, une ingérence au droit au respect de sa correspondance. Elle relève en outre que ladite ingérence est antérieure au 23 septembre 1998, date à laquelle la Cour a estimé dans l'arrêt Petra précité que l'article 8 de la Convention avait été méconnu par les autorités au motif que les dispositions internes applicables ne satisfaisaient pas aux exigences du paragraphe 2 l'article 8 de la Convention (Petra, précité, §§ 38-39).

41. Or, l'ingérence litigieuse étant fondée en l'occurrence sur les mêmes dispositions internes que celles déjà jugées comme ne répondant pas aux exigences d'une « loi », la Cour conclut que rien en l'espèce ne permet de distinguer de ce point de vue la présente affaire de l'affaire Petra précitée.

42. Partant, l'ingérence litigieuse n'étant pas prévue par une « loi », la Cour conclut qu'il y a eu violation de l'article 8 de la Convention de ce chef.

2. La période après le 24 novembre 1997

43. Pour ce qui est du respect du secret de la correspondance du requérant après le 24 novembre 1997, la Cour se voit placée devant une controverse entre les parties, dans la mesure où le Gouvernement nie l'existence de toute ingérence après la date à laquelle le ministre de la justice a adopté l'arrêté garantissant le secret de la correspondance des détenus, fait contesté par le requérant. Dans ces circonstances, il incombe tout d'abord à la Cour de trancher cette controverse sur la base de l'ensemble du dossier en sa possession (Messina c. Italie, arrêt du 2 février 1993, série A no 257‑H, § 31)

44. La Cour relève qu'il résulte de la lettre du 15 mai 2002 de la direction du pénitencier de Mărgineni que les autorités de cet établissement ont continué, même après le 24 novembre 1997, de contrôler la correspondance du requérant, en particulier son objet et ses destinataires. Elle note à cet égard que les autorités pénitentiaires étaient au courant de ce que qu'entre 1998 et 2002, le requérant n'avait pas envoyé de requête à la Cour et qu'il avait envoyé une seule demande au ministre de la Justice pour demander la grâce (paragraphe 26 ci-dessus). Plus encore, elle note que le requérant s'est plaint dans sa lettre du 11 novembre 2000 que celle du Greffe de la Cour du 27 octobre 2000 lui était parvenue ouverte, fait que le Gouvernement ne conteste pas (paragraphe 25 ci-dessus).
Ces éléments permettent à la Cour d'ajouter foi aux allégations de l'intéressé. Elle estime donc que l'ingérence au droit au respect du secret de sa correspondance a continué même après la date de l'adoption de l'arrêté du ministre garantissant le secret de la correspondance de détenus.

45. Cette ingérence emporte violation de l'article 8 de la Convention, à moins qu'elle ne soit « prévue par la loi », qu'elle poursuive un ou des buts légitimes au regard du paragraphe 2 et, qu'elle soit, de plus, « nécessaire, dans une société démocratique », pour les atteindre (voir les arrêts Silver et autres c.. Royaume-Uni du 25 mars 1992, série A no 233, p. 16, § 34, et Calogero Royaume-Uni du 25 mars 1983, série A no 61, p. 32, § 84, Campbell c Diana c. Italie du 15 novembre 1996, Recueil 1996-V, p. 1775, § 28).

46. S'agissant de la légalité de l'ingérence, la Cour, en l'absence d'indications plus précises fournies par les parties, part de l'idée que le contrôle de la correspondance du requérant s'est fondé, à la différence de l'affaire Petra précitée, sur l'arrêté que le ministre de la Justice aurait adopté le 24 novembre 1997, garantissant le secret de la correspondance des détenus. A supposer que tel n'était pas le cas, il appartenait au Gouvernement défendeur d'indiquer la disposition de loi éventuelle sur laquelle s'étaient appuyées les autorités nationales pour soumettre à contrôle la correspondance du détenu (Di Giovine c. Italie, no 39920/98, § 25, arrêt du 26 juillet 2001, non publié).

47. Or, la Cour relève tout d'abord certaines incohérences dans les observations du Gouvernement à l'égard de l'arrêté du 24 novembre 1997, dans la mesure où celui-ci est parfois identifié sous le no 2036/C, parfois sous le no 2037/C. De surcroît, il ne résulte nullement des éléments fournis par le Gouvernement ou que la Cour a pu se procurer d'elle-même que l'arrêté en question a été publié. Dans ces conditions, et à la lumière de sa jurisprudence en la matière (Petra, précité, § 37 ; Di Giovine, précité, § 26 ; Peers c. Grèce, no 28524/95, § 82, CEDH 2001‑III et Labita c. Italie [GC], no 26772/95, §§ 175‑185, CEDH 2000‑IV), la Cour estime que l'ingérence litigieuse n'était pas prévue par une « loi », au sens du paragraphe 2 de l'article 8 de la Convention.

48. Eu égard à la conclusion qui précède, la Cour n'estime pas nécessaire de vérifier en l'espèce le respect des autres exigences du paragraphe 2 de l'article 8 et conclut à la violation de l'article 8 de la Convention.

3. Sur le refus de l'administration du pénitencier de fournir au requérant le nécessaire pour sa correspondance avec la Cour

B. Appréciation de la Cour

56. La Cour note que ce grief du requérant pose en l'espèce deux questions distinctes, bien qu'étroitement liées entre elles : celle, tout d'abord, de savoir si l'Etat avait une obligation positive de fournir au requérant le nécessaire pour sa correspondance avec la Cour ; celle, ensuite, et le cas échéant, de savoir si l'Etat a manqué à une telle obligation.

1. Sur la responsabilité de l'Etat pour manquement à une obligation positive

57. La Cour note que le requérant se plaint en substance non pas d'un acte, mais de l'inaction de l'Etat. Elle rappelle à cet égard que, si l'article 8 a essentiellement pour objet de prémunir l'individu contre les ingérences arbitraires des pouvoirs publics, il ne se contente pas de commander à l'Etat de s'abstenir de pareilles ingérences : à cet engagement négatif peuvent s'ajouter des obligations positives inhérentes à un respect effectif des droits gratis par l'article 8 précité (X et Y c. Pays-Bas, arrêt du 26 mars 1985, série A no 91, p. 11, § 23, et Stjerna c. Finlande, arrêt du 25 novembre 1994, série A no 299-B, p. 61, § 38).

58. Sur le terrain de l'article 8 de la Convention, la Cour a conclu à l'existence de ce type d'obligations à la charge d'un Etat lorsqu'elle a constaté la présence d'un lien direct et immédiat entre, d'une part, les mesures demandées par un requérant et, d'autre part, la vie privée et/ou familiale de celui-ci (voir, parmi d'autres, López Ostra c. Espagne, arrêt du 9 décembre 1994, série A no 303-C, p. 56, § 58 ; Guerra et autres c. Italie, arrêt du 19 février 1998, Recueil 1998-I, p. 228, § 60).

59. En l'espèce, la Cour constate qu'un tel lien direct existe entre le droit revendiqué par le requérant, à savoir celui de se voir octroyer, par l'administration de la prison, des fournitures nécessaires pour sa correspondance avec la Cour, et, d'autre part, le droit du requérant au respect de sa correspondance, tel que garanti par l'article 8 de la Convention. En effet, le fait de disposer de fournitures comme du papier à écrire, des timbres et des enveloppes est inhérent à l'exercice, par le requérant, de son droit au respect de sa correspondance, garanti par l'article 8. Il incombe dès lors à la Cour d'examiner si les autorités ont manqué à l'obligation positive alléguée par le requérant.

2. Sur la question de savoir si l'Etat a manqué à son obligation positive

60. La Cour estime que, contrairement aux affirmations du Gouvernement, les allégations du requérant formant cette troisième branche de son grief sous l'angle de l'article 8 ne sont pas dépourvues de fondement. En effet, elle relève que plusieurs lettres du requérant sont arrivées dans des enveloppes des autres détenus et que le requérant a constamment informé la Cour à ce sujet, lui demandant son aide (paragraphes 23-24 ci-dessus).

61. La Cour rappelle à cet égard que l'article 8 de la Convention n'oblige pas les Etats à supporter les frais d'affranchissement de toute la correspondance des détenus, ni ne garantit aux détenus le choix du

		matériel à écrire (Boyle c. Royaume-Uni, no 9659/82, décision de la Commission du 6 mars 1985, Décisions et rapports 41, p. 91 et Farrant c. Royaume-Uni, no 7291/75, décision de la Commission du 18 octobre 1985, D.R. 50, p. 5). Toutefois, un problème pourrait surgir si, faute de moyens financiers, la correspondance d'un détenu a sérieusement été entravée (Boyle, précitée). De même, l'obligation faite aux détenus d'utiliser pour leur correspondance le papier réglementaire de la prison ne constitue pas une ingérence dans le droit au respect de la correspondance, pourvu que ce papier soit immédiatement disponible (Farrant, précitée). 62. La Cour note que le Gouvernement, après avoir fait allusion à une réglementation en vertu de laquelle le requérant pourrait bénéficier de deux enveloppes gratuites par mois, a été en défaut de faire la preuve que ce dernier en aurait effectivement bénéficié. 63. Plus encore, elle souscrit à l'argument de la partie requérante selon lequel les enveloppes ne sont pas suffisantes pour pouvoir exercer son droit à la correspondance. Or, la Cour note que, d'après le requérant, toutes ses demandes de fournitures, adressées oralement auprès du commandant de la prison, ont été rejetées au motif que seules des enveloppes affranchies pour la Roumanie, et non pas pour l'étranger, étaient disponibles, fait que le Gouvernement ne conteste pas. 64. La Cour ne saurait accueillir davantage l'argument du Gouvernement selon lequel le requérant aurait omis de faire une demande écrite, dans la mesure où l'intéressé visait précisément l'obtention, parmi d'autres fournitures, du papier à écrire. 65. Dans ces circonstances, la Cour estime que les autorités ont manqué à leur obligation positive de fournir au requérant le nécessaire pour sa correspondance avec la Cour et que, dès lors, il y a eu violation de l'article 8 de la Convention de ce chef.
23.	Eur. Court HR *Hewitson v. the United Kingdom*, judgment of 27 May 2003, 50015/99: recording devices; secret surveillance	20. The Government accepted, following the judgment in Khan v. the United Kingdom (no. 35394/97, ECHR 2000-V, §§ 26-28) that the use of the recording device amounted to an interference with the applicant's right to private life under Article 8 § 1 of the Convention and that the measures were not used "in accordance with law" within the meaning of Article 8 § 2 of the Convention. 21. **The Court recalls, as in the above-mentioned Khan case, that at the relevant time there existed no statutory system to regulate the use of covert recording devices by the police. The interferences disclosed by the measures implemented in respect of the applicant were therefore not "in accordance with the law" as required by the second paragraph of Article 8 and there has accordingly been a violation of this provision.**
24.	Eur. Court HR, *Chalkley v. the United Kingdom* judgment of 12 June 2003, 63831/00: recording device; secret surveillance	24. The Government accepted, following the judgment in Khan v. the United Kingdom (no. 35394/97, ECHR 2000-V, §§ 26-28), that the use of the recording device amounted to an interference with the applicant's right to private life under Article 8 § 1 and that the measures were not used "in accordance with law" within the meaning of Article 8 § 2. 25. **The Court recalls, as in the above-mentioned Khan case, that at the relevant time there existed no statutory system to regulate the use of covert recording devices by the police. The interference disclosed by the measures implemented in respect of the applicant were therefore not "in accordance with the law" as required by the**

		second paragraph of Article 8 and there has accordingly been a violation of Article 8.
25.	Eur. Court HR, *A. v. the United Kingdom* judgment of 17 July 2003, 63737/00: video surveillance; security cameras; quality of the law	36. **Private life is a broad term not susceptible to exhaustive definition. Aspects such as gender identification, name, sexual orientation and sexual life are important elements of the personal sphere protected by Article 8. The Article also protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world and it may include activities of a professional or business nature. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life" (P.G. and J.H. v. the United Kingdom, no. 44787/98, § 56, ECHR 2001-IX, with further references).** 37. **It cannot therefore be excluded that a person's private life may be concerned in measures effected outside a person's home or private premises. A person's reasonable expectations as to privacy is a significant though not necessarily conclusive factor (P.G. and J.H v. United Kingdom, § 57).** 38. **The monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life (see, for example, Herbecq and Another v. Belgium, applications nos. 32200/96 and 32201/96, Commission decision of 14 January 1998, DR 92-A, p. 92). On the other hand, the recording of the data and the systematic or permanent nature of the record may give rise to such considerations (see, for example, Rotaru v. Romania [GC], no. 28341/95, §§ 43-44, ECHR 2000-V, and Amann v. Switzerland [GC], no. 27798/95, §§ 65-67, ECHR 2000-II, where the compilation of data by security services on particular individuals even without the use of covert surveillance methods constituted an interference with the applicants' private lives). While the permanent recording of the voices of P.G. and J.H. was made while they answered questions in a public area of a police station as police officers listened to them, the recording of their voices for further analysis was regarded as the processing of personal data about them amounting to an interference with their right to respect for their private lives (the above-cited P.G. and J.H. judgment, at §§ 59-60). Publication of the material in a manner or degree beyond that normally foreseeable may also bring security recordings within the scope of Article 8 § 1. In Peck v. the United Kingdom (no. 44647/98, judgment of 28 January 2003, ECHR 2003-...), the disclosure to the media for broadcast use of video footage of the applicant whose suicide attempt was caught on close circuit television cameras was found to be a serious interference with the applicant's private life, notwithstanding that he was in a public place at the time.** 39. In the present case, the applicant was filmed on video in the custody suite of a police station. The Government argued that this could not be regarded as a private place, and that as the cameras which were running for security purposes were visible to the applicant he must have realised that he was being filmed, with no reasonable expectation of privacy in the circumstances. 40. **As stated above, the normal use of security cameras per se whether in the public street or on premises, such as shopping centres or police stations where they serve a legitimate and foreseeable purpose, do not raise issues under Article 8 § 1 of the Convention.**

Here, however, the police regulated the security camera so that it could take clear footage of the applicant in the custody suite and inserted it in a montage of film of other persons to show to witnesses for the purposes of seeing whether they identified the applicant as the perpetrator of the robberies under investigation. The video was also shown during the applicant's trial in a public court room. The question is whether this use of the camera and footage constituted a processing or use of personal data of a nature to constitute an interference with respect for private life.

41. **The Court recalls that the applicant had been brought to the police station to attend an identity parade and that he had refused to participate. Whether or not he was aware of the security cameras running in the custody suite, there is no indication that the applicant had any expectation that footage was being taken of him within the police station for use in a video identification procedure and, potentially, as evidence prejudicial to his defence at trial. This ploy adopted by the police went beyond the normal or expected use of this type of camera, as indeed is demonstrated by the fact that the police were required to obtain permission and an engineer had to adjust the camera. The permanent recording of the footage and its inclusion in a montage for further use may therefore be regarded as the processing or collecting of personal data about the applicant.**

42. The Government argued that the use of the footage was analogous to the use of photos in identification albums, in which circumstance the Commission had stated that no issue arose where they were used solely for the purpose of identifying offenders in criminal proceedings (Lupker v. the Netherlands, no. 18395/91, Commission decision of 7 December 1992, unreported). However, the Commission emphasised in that case that the photographs had not come into the possession of the police through any invasion of privacy, the photographs having been submitted voluntarily to the authorities in passport applications or having been taken by the police on the occasion of a previous arrest. The footage in question in the present case had not been obtained voluntarily or in circumstances where it could be reasonably anticipated that it would be recorded and used for identification purposes.

43. **The Court considers therefore that the recording and use of the video footage of the applicant in this case discloses an interference with his right to respect for private life**

45. **The expression "in accordance with the law" requires, firstly, that the impugned measure should have some basis in domestic law; secondly, it refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and that it is compatible with the rule of law (see, amongst other authorities, Kopp v. Switzerland, judgment of 25 March 1998, Reports 1998-II, p. 540, § 55). It also requires that the measure under examination comply with the requirements laid down by the domestic law providing for the interference.**

48. Though the Government have argued that it was the quality of the law that was important and that the trial judge ruled that it was not unfair for the videotape to be used in the trial, the Court would note that the safeguards relied on by the Government as demonstrating the requisite statutory protection were, in the circumstances, flouted by the police. Issues relating to the fairness of the use of the evidence in the trial must also be distinguished from the question of lawfulness of the interference

		with private life and are relevant rather to Article 6 than to Article 8. It recalls in this context its decision on admissibility of 26 September 2002 in which it rejected the applicant's complaints under Article 6, observing that the obtaining of the film in this case was a matter which called into play the Contracting State's responsibility under Article 8 to secure the right to respect for private life in due form. 49. **The interference was not therefore "in accordance with the law" as required by the second paragraph of Article 8 and there has been a violation of this provision.** In these circumstances, an examination of the necessity of the interference is not required.
26.	Eur. Court HR, *Lewis v. the United Kingdom*, judgment of 25 November 2003, 1303/02: recording devices; secret surveillance	18. The Government conceded, in the light of Khan v. the United Kingdom (no. 35394/97, ECHR 2000-V, §§ 26-28), that the installation of a recording device in the applicant's home by the police amounted to an interference with the applicant's right to private life guaranteed by Article 8 and that these measures were not "in accordance with the law" for the purposes of Article 8 § 2. 19. **The Court recalls, as in the above-mentioned Khan case, that at the relevant time there existed no statutory system to regulate the use of covert recording devices by the police. The interference disclosed by the measures implemented in respect of the applicant were therefore not "in accordance with the law" as required by the second paragraph of Article 8 and there has accordingly been a violation of Article 8.**
27.	Eur. Court HR, *Matwiejczuk v. Poland* judgment of 2 December 2003, 37641/97: monitoring of correspondence; quality of the law	98. **The expression "in accordance with the law" requires that the interference in question must have some basis in domestic law. A law must be adequately accessible: the citizen must be able to have an indication that is adequate, in the circumstances, of the legal rules applicable to a given case. Moreover, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail. Finally, a law which confers discretion must indicate the scope of that discretion. However, the Court has recognised the impossibility of attaining absolute certainty in the framing of laws and the risk that the search for certainty may entail excessive rigidity (see, among other authorities, Silver and Others v. the United Kingdom, judgment of 25 March 1983, Series A no. 61, p. 33, §§ 86-88).** 99. The Court notes that an envelope mailed to the applicant on 23 February 1999 bears a stamp: "Censored on, signature" (Ocenzurowano dn. podpis), a hand-written date: 5 March and an illegible signature (see paragraph 58 above). It considers that even if there is no separate stamp on the letter as such, there is, in the particular circumstances of the case, a reasonable likelihood that the envelope was opened by the domestic authorities. In coming to such a conclusion, the Court takes into account that, in the Polish language, the word ocenzurowano means that a competent authority, after having controlled the content of a particular communication, decides to allow its delivery or expedition. Consequently, as long as the domestic authorities continue the practice of marking the detainees' letters with a simple ocenzurowano stamp, the Court would have no alternative but to presume that those letters have been opened and their contents read. It is the matter for the domestic authorities, to elaborate a procedure of giving clearance for delivery and expedition of letters to and from the European Court of Human Rights in a way clearly indicating that neither the relevant envelopes have been opened nor the

		letters have been read. The Court would also point out that the risk of such a stamp being forged by prisoners in order to fabricate evidence in the Strasbourg proceedings is so negligible that it must be discounted. Had domestic authorities been concerned about the risk of fabrication, they could have avoided it by adding to the register of incoming mail information about its condition (see, mutatis mutandis, Campbell v. the United Kingdom, judgment of 28 February 1992, Series A no. 233, p. 22, § 62; Halford v. the United Kingdom, judgment of 25 June 1997, Reports of Judgments and Decisions 1997-III, p. 1016, § 48). 100. **It follows that the monitoring of the Court's correspondence addressed to the applicant constituted an "interference by a public authority", within the meaning of Article 8 § 2, with the exercise of the applicant's right to respect for his correspondence.** 102. The Court further notes that § 37 (4) of the Rules of Detention on Remand 1998 requires that the inspection of detainee's correspondence take place in his presence (see paragraph 66 above). In the present case the Government failed to present any evidence rebutting the applicant's claim that the opening of the Court's letter of 23 February 1999 had not taken place in his presence. It follows that the opening of the letter was not "in accordance with the law". There has therefore been a breach of Article 8 of the Convention.
28.	Eur. Court HR *Doerga v. Netherlands*, judgment of 27 April, 200450210/99: interception of telephone conversations; secret surveillance; quality of the law; foreseeability; protection against arbitrary interference	45. **The expression "in accordance with the law" requires, firstly, that the impugned measure should have some basis in domestic law; secondly, it refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and that it is compatible with the rule of law (see Kopp v. Switzerland, judgment of 25 March 1998, Reports of Judgments and Decisions 1998-II, p. 540, § 55, and Amann v. Switzerland [GC], no. 27798/95, § 50, ECHR 2000-II). In the context of interception of communications by public authorities, because of the lack of public scrutiny and the risk of misuse of power, the domestic law must provide some protection to the individual against arbitrary interference with the rights protected by Article 8 of the Convention (see, Halford v. the United Kingdom, judgment of 25 June 1997, Reports 1997-III, p. 1017, § 49).** 50. **A rule is "foreseeable" if it is formulated with sufficient precision to enable the person concerned - if need be with appropriate advice - to regulate his conduct. In the cases of Kruslin v. France and Huvig v. France (judgments of 24 April 1990, Series A no. 176-A and B, pp. 22-23, § 30, and pp. 54-55, § 29) the Court has underlined the importance of that concept in the following terms:** **"It implies that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by paragraph 1 [of Article 8]. Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident. Undoubtedly, the requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations or judicial investigations, as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and**

		the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence. In its judgment of 25 March 1983 in the case of Silver and Others, the Court held that "a law which confers a discretion must indicate the scope of that discretion", although the detailed procedures and conditions to be observed do not necessarily have to be incorporated in rules of substantive law (Series A no. 61, pp. 33-34, §§ 88-89). The degree of precision required of the "law" in this connection will depend upon the particular subject-matter. Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference." **Furthermore, tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a 'law' that is particularly precise. It is essential to have clear, detailed rules on the subject (see, Kruslin v. France and Huvig v. France, cited above, p. 23, § 33, and p. 55, § 32, and Amann v. Switzerland, cited above, § 56).** 52. The Court finds that the rules at issue in the present case are lacking both in clarity and detail in that neither circular no. 1183/379 nor the internal regulations of the Marwei penitentiary give any precise indication as to the circumstances in which prisoners' telephone conversations may be monitored, recorded and retained by penitentiary authorities or the procedures to be observed. This is illustrated by the fact that the domestic courts interpreted the applicable internal rule that "the tapes are not retained and [must be] erased immediately" (see paragraph 22 above) in such a manner that recordings of intercepted telephone conversations can be retained for as long as the danger giving rise to the recording exists (see paragraph 17 above), which in the instant case amounted to a period of more than eight months (see paragraphs 8-10 and 14 above). 53. **Although the Court accepts, having regard to the ordinary and reasonable requirements of imprisonment, that it may be necessary to monitor detainees' contacts with the outside world, including contacts by telephone, it does not find that the rules at issue can be regarded as being sufficiently clear and detailed to afford appropriate protection against arbitrary interference by the authorities with the applicant's right to respect for his private life and correspondence.** 54. The interference complained of was not therefore "in accordance with the law" as required by the second paragraph of Article 8 and there has been a violation of this provision. In these circumstances, an examination of the necessity of the interference is not required.
29.	Eur. Court HR, *Von Hannover v. Germany* judgment of 24 June 2004, 59320/00: photos; tabloid press; freedom of expression; legitimate expectation of privacy	50. **The Court reiterates that the concept of private life extends to aspects relating to personal identity, such as a person's name (see Burghartz v. Switzerland, judgment of 22 February 1994, Series A no. 280-B, p. 28, § 24), or a person's picture (see Schüssel v. Austria (dec.), no. 42409/98, 21 February 2002).** **Furthermore, private life, in the Court's view, includes a person's physical and psychological integrity; the guarantee afforded by Article 8 of the Convention is primarily intended to ensure the**

development, without outside interference, of the personality of each individual in his relations with other human beings (see, mutatis mutandis, Niemietz v. Germany, judgment of 16 December 1992, Series A no. 251-B, p. 33, § 29, and Botta v. Italy, judgment of 24 February 1998, Reports of Judgments and Decisions 1998-I, p. 422, § 32). There is therefore a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life" (see, mutatis mutandis, P.G. and J.H. v. the United Kingdom, no. 44787/98, § 56, ECHR 2001-IX, and Peck v. the United Kingdom, no. 44647/98, § 57, ECHR 2003-I.).

51. **The Court has also indicated that, in certain circumstances, a person has a "legitimate expectation" of protection and respect for his or her private life. Accordingly, it has held in a case concerning the interception of telephone calls on business premises that the applicant "would have had a reasonable expectation of privacy for such calls" (see Halford v. the United Kingdom, judgment of 25 June 1997, Reports 1997-III, p.1016, § 45).**

53. In the present case there is no doubt that the publication by various German magazines of photos of the applicant in her daily life either on her own or with other people falls within the scope of her private life.

57. **The Court reiterates that although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves (see, mutatis mutandis, X and Y v. the Netherlands, judgment of 26 March 1985, Series A no. 91, p. 11, § 23; Stjerna v. Finland, judgment of 25 November 1994, Series A no. 299-B, p. 61, § 38; and Verliere v. Switzerland (dec.), no. 41953/98, ECHR 2001-VII). That also applies to the protection of a person's picture against abuse by others (see Schüssel, cited above). The boundary between the State's positive and negative obligations under this provision does not lend itself to precise definition. The applicable principles are, nonetheless, similar. In both contexts regard must be had to the fair balance that has to be struck between the competing interests of the individual and of the community as a whole; and in both contexts the State enjoys a certain margin of appreciation (see, among many other authorities, Keegan v. Ireland, judgment of 26 May 1994, Series A no. 290, p. 19, § 49, and Botta, cited above, p. 427, § 33).**

58. **That protection of private life has to be balanced against the freedom of expression guaranteed by Article 10 of the Convention. In that context the Court reiterates that the freedom of expression constitutes one of the essential foundations of a democratic society. Subject to paragraph 2 of Article 10, it is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no "democratic society" (see Handyside v. the United Kingdom, judgment of 7 December 1976, Series A no. 24, p. 23, § 49). In that connection the press plays an essential role in a democratic society. Although it must not overstep certain bounds, in particular in respect of the reputation and rights of others, its duty is nevertheless**

to impart – in a manner consistent with its obligations and responsibilities – information and ideas on all matters of public interest (see, among many authorities, Observer and Guardian v. the United Kingdom, judgment of 26 November 1991, Series A no. 216, p. 29-30, § 59, and Bladet Tromsø and Stensaas v. Norway [GC], no. 21980/93, § 59, ECHR 1999-III). Journalistic freedom also covers possible recourse to a degree of exaggeration, or even provocation (see Prager and Oberschlick v. Austria, judgment of 26 April 1995, Series A no. 313, p. 19, § 38; Tammer v. Estonia, no. 41205/98, § 59-63, ECHR 2001-I; and Prisma Press v. France (dec.), nos. 66910/01 and 71612/01, 1 July 2003).

59. **Although freedom of expression also extends to the publication of photos, this is an area in which the protection of the rights and reputation of others takes on particular importance. The present case does not concern the dissemination of "ideas", but of images containing very personal or even intimate "information" about an individual. Furthermore, photos appearing in the tabloid press are often taken in a climate of continual harassment which induces in the person concerned a very strong sense of intrusion into their private life or even of persecution.**

60. **In the cases in which the Court has had to balance the protection of private life against the freedom of expression it has always stressed the contribution made by photos or articles in the press to a debate of general interest (see, as a recent authority, News Verlags GmbH & CoKG v. Austria, no. 31457/96, § 52 et seq., ECHR 2000-I, and Krone Verlag GmbH & Co. KG v. Austria, no. 34315/96, § 33 et seq., 26 February 2002). The Court thus found, in one case, that the use of certain terms in relation to an individual's private life was not "justified by considerations of public concern" and that those terms did not "[bear] on a matter of general importance" (see Tammer, cited above, § 68) and went on to hold that there had not been a violation of Article 10. In another case, however, the Court attached particular importance to the fact that the subject in question was a news item of "major public concern" and that the published photographs "did not disclose any details of [the] private life" of the person in question (see Krone Verlag, cited above, § 37) and held that there had been a violation of Article 10. Similarly, in a recent case concerning the publication by President Mitterand's former private doctor of a book containing revelations about the President's state of health, the Court held that "the more time passed the more the public interest in President Mitterand's two seven-year presidential terms prevailed over the requirements of the protection of his rights with regard to medical confidentiality" (see Plon (Société) v. France, no. 58148/00, 18 May 2004) and held that there had been a breach of Article 10.**

c. Application of these general principles by the Court

61. The Court points out at the outset that in the present case the photos of the applicant in the various German magazines show her in scenes from her daily life, thus engaged in activities of a purely private nature such as practising sport, out walking, leaving a restaurant or on holiday. The photos, in which the applicant appears sometimes alone and sometimes in company, illustrate a series of articles with such anodyne titles as 'Pure happiness", "Caroline ... a woman returning to life", "Out and about with Princess Caroline in Paris" and "The kiss. Or: they are not hiding anymore ..." (see paragraphs 11-17 above).

62. The Court also notes that the applicant, as a member of the Prince of Monaco's family, represents the ruling family at certain cultural or charitable events. However, she does not exercise any function within or on behalf of the State of Monaco or one of its institutions (see paragraph 8 above).

63. **The Court considers that a fundamental distinction needs to be made between reporting facts – even controversial ones – capable of contributing to a debate in a democratic society relating to politicians in the exercise of their functions, for example, and reporting details of the private life of an individual who, moreover, as in this case, does not exercise official functions. While in the former case the press exercises its vital role of "watchdog" in a democracy by contributing to "impart[ing] information and ideas on matters of public interest (Observer and Guardian, cited above, ibid.) it does not do so in the latter case.**

64. **Similarly, although the public has a right to be informed, which is an essential right in a democratic society that, in certain special circumstances, can even extend to aspects of the private life of public figures, particularly where politicians are concerned (see Plon (Société), cited above, ibid.), this is not the case here. The situation here does not come within the sphere of any political or public debate because the published photos and accompanying commentaries relate exclusively to details of the applicant's private life.**

65. **As in other similar cases it has examined, the Court considers that the publication of the photos and articles in question, of which the sole purpose was to satisfy the curiosity of a particular readership regarding the details of the applicant's private life, cannot be deemed to contribute to any debate of general interest to society despite the applicant being known to the public (see, mutatis mutandis, Jaime Campmany y Diez de Revenga and Juan Luís Lopez-Galiacho Perona v. Spain (dec.), no. 54224/00, 12 December 2000; Julio Bou Gibert and El Hogar Y La Moda J.A. v. Spain (dec.), no. 14929/02, 13 May 2003; and Prisma Presse, cited above).**

66. **In these conditions freedom of expression calls for a narrower interpretation (see Prisma Presse, cited above, and, by converse implication, Krone Verlag, cited above, § 37).**

67. **In that connection the Court also takes account of the resolution of the Parliamentary Assembly of the Council of Europe on the right to privacy, which stresses the "one-sided interpretation of the right to freedom of expression" by certain media which attempt to justify an infringement of the rights protected by Article 8 of the Convention by claiming that "their readers are entitled to know everything about public figures" (see paragraph 42 above, and Prisma Presse, cited above).**

68. **The Court finds another point to be of importance: even though, strictly speaking, the present application concerns only the publication of the photos and articles by various German magazines, the context in which these photos were taken – without the applicant's knowledge or consent – and the harassment endured by many public figures in their daily lives cannot be fully disregarded (see paragraph 59 above).**
In the present case this point is illustrated in particularly striking fashion by the photos taken of the applicant at the Monte Carlo Beach Club

tripping over an obstacle and falling down (see paragraph 17 above). It appears that these photos were taken secretly at a distance of several hundred metres, probably from a neighbouring house, whereas journalists and photographers' access to the club was strictly regulated (see paragraph 33 above).

69. **The Court reiterates the fundamental importance of protecting private life from the point of view of the development of every human being's personality. That protection – as stated above – extends beyond the private family circle and also includes a social dimension. The Court considers that anyone, even if they are known to the general public, must be able to enjoy a "legitimate expectation" of protection of and respect for their private life (see paragraph 51 above and, mutatis mutandis, Halford, cited above, § 45).**

70. **Furthermore, increased vigilance in protecting private life is necessary to contend with new communication technologies which make it possible to store and reproduce personal data (see point 5 of the Parliamentary Assembly's resolution on the right to privacy – see paragraph 42 above and, mutatis mutandis, Amann v. Switzerland [GC], no. 27798/95, § 65-67, ECHR 2000-II; Rotaru v. Romania [GC], no. 28341/95, § 43-44, ECHR 2000-V; P.G. and J.H., cited above, § 57-60, ECHR 2001-IX; and Peck, cited above, §§ 59-63, and § 78). This also applies to the systematic taking of specific photos and their dissemination to a broad section of the public.**

71. **Lastly, the Court reiterates that the Convention is intended to guarantee not rights that are theoretical or illusory but rights that are practical and effective (see Artico v. Italy, judgment of 13 May 1980, Series A no. 37, p. 15-16, § 33).**

72. The Court has difficulty in agreeing with the domestic courts' interpretation of section 23(1) of the Copyright (Arts Domain) Act, which consists in describing a person as such as a figure of contemporary society "par excellence". Since that definition affords the person very limited protection of their private life or the right to control the use of their image, it could conceivably be appropriate for politicians exercising official functions. However, it cannot be justified for a "private" individual, such as the applicant, in whom the interest of the general public and the press is based solely on her membership of a reigning family whereas she herself does not exercise any official functions.
In any event the Court considers that, in these conditions, the Act has to be interpreted narrowly to ensure that the State complies with its positive obligation under the Convention to protect private life and the right to control the use of one's image.

73. Lastly, the distinction drawn between figures of contemporary society "par excellence" and "relatively" public figures has to be clear and obvious so that, in a state governed by the rule of law, the individual has precise indications as to the behaviour he or she should adopt. Above all, they need to know exactly when and where they are in a protected sphere or, on the contrary, in a sphere in which they must expect interference from others, especially the tabloid press.

74. **The Court therefore considers that the criteria on which the domestic courts based their decisions were not sufficient to protect the applicant's private life effectively. As a figure of contemporary society "par excellence" she cannot – in the name of freedom of the press and the public interest – rely on protection of her private life unless she is in a secluded place out of the public eye and, moreover,**

		succeeds in proving it (which can be difficult). Where that is not the case, she has to accept that she might be photographed at almost any time, systematically, and that the photos are then very widely disseminated even if, as was the case here, the photos and accompanying articles relate exclusively to details of her private life. 75. **In the Court's view, the criterion of spatial isolation, although apposite in theory, is in reality too vague and difficult for the person concerned to determine in advance. In the present case merely classifying the applicant as a figure of contemporary society "par excellence" does not suffice to justify such an intrusion into her private life.** 76. **As the Court has stated above, it considers that the decisive factor in balancing the protection of private life against freedom of expression should lie in the contribution that the published photos and articles make to a debate of general interest. It is clear in the instant case that they made no such contribution since the applicant exercises no official function and the photos and articles related exclusively to details of her private life.** 77. **Furthermore, the Court considers that the public does not have a legitimate interest in knowing where the applicant is and how she behaves generally in her private life even if she appears in places that cannot always be described as secluded and despite the fact that she is well known to the public.** **Even if such a public interest exists, as does a commercial interest of the magazines in publishing these photos and these articles, in the instant case those interests must, in the Court's view, yield to the applicant's right to the effective protection of her private life.** 78. **Lastly, in the Court's opinion the criteria established by the domestic courts were not sufficient to ensure the effective protection of the applicant's private life and she should, in the circumstances of the case, have had a "legitimate expectation" of protection of her private life.** 79. **Having regard to all the foregoing factors, and despite the margin of appreciation afforded to the State in this area, the Court considers that the German courts did not strike a fair balance between the competing interests.** 80. There has therefore been a breach of Article 8 of the Convention.
30.	Eur. Court HR, *Wood v. the United Kingdom* judgment of 16 November 2004, 23414/02: secret surveillance; effective remedy	32. **The Government conceded, in light of the Court's case-law, that there had been no legal basis for the measures and that there was no effective remedy under domestic law for that breach of Article 8.** 33. **The Court accordingly finds that the covert surveillance measures involving the applicant constituted an interference which was not "in accordance with the law" and was in breach of Article 8 of the Convention;** furthermore, there has been a breach of Article 13 of the Convention (see, amongst other authorities, Khan v. the United Kingdom, no. 35394/97, §§ 26 and 47, ECHR 2000-V; Taylor-Sabori v. the United Kingdom, no. 47114/99, judgment of 22 October 2002, §§ 19 and 23.
31.	Eur. Court HR, *Sciacca v. Italy*, judgment of 11 January 2005, 50774/99: publication	27. **The Court has already examined the question of the publication of photographs of public figures (see Von Hannover v. Germany, no. 59320/00, § 50, ECHR 2004-VI) or politicians (see Schüssel v. Austria (dec.), no. 42409/98, 21 February 2002). After concluding that the**

	of photos; criminal proceedings; press	**publication of photographs fell within the scope of private life, it examined the question of the respondent State's compliance with the positive obligations incumbent on it when the publication was not the result of action or co-operation on the part of State bodies.** 28. The present case differs from previous ones in that the applicant was not someone who featured in a public context (public figure or politician) but the subject of criminal proceedings. Furthermore, the published photograph, which had been taken for the purposes of an official file, had been given to the press by the Revenue Police (see paragraphs 16 and 26 above). That being so, in accordance with its case-law the Court must determine whether the respondent State complied with its obligation not to interfere with the applicant's right to respect for her private life. It must verify whether there has been an interference with that right in the present case and, if so, whether that interference satisfied the conditions laid down in the second paragraph of Article 8: was it "in accordance with the law", did it pursue one or more legitimate aims under paragraph 2 of that Article and was it "necessary in a democratic society" to achieve them? 29. **Regarding whether there has been an interference, the Court reiterates that the concept of private life includes elements relating to a person's right to their image and that the publication of a photograph falls within the scope of private life (see Von Hannover, cited above, §§ 50-53). It has also given guidelines regarding the scope of private life and found that there is "a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life' " (ibid.). In the instant case the applicant's status as an "ordinary person" enlarges the zone of interaction which may fall within the scope of private life, and the fact that the applicant was the subject of criminal proceedings cannot curtail the scope of such protection.** **Accordingly, the Court concludes that there has been interference.** 30. **As regards compliance with the condition that the interference must be "in accordance with the law", the Court notes that the applicant argued that this condition had not been complied with and that her submission was not disputed by the Government. According to the information available to it, the Court considers that the subject matter was not governed by a "law" that satisfied the criteria laid down by the Court's case-law, but rather by practice. The Court also notes that the exception to the secrecy rule regarding measures taken during preliminary investigations, provided for in Article 329 § 2 of the CCP, concerns only cases where an investigative document is published for the purposes of continuing the investigation. That was not the case here, however.** **The Court therefore concludes that the interference has not been shown to have been in accordance with the law. That finding is sufficient for the Court to conclude that there has been a breach of Article 8. Accordingly, it is not necessary to determine whether the interference in question pursued a "legitimate aim" or was "necessary in a democratic society" to achieve that aim (see M. v. the Netherlands, no. 39339/97, § 46, 8 April 2003).** 31. In conclusion, there has been a violation of Article 8 of the Convention.
32.	Eur. Court HR, *Pisk-Piskowski v. Poland* judgment of 14 January 2005, 92/03: interference of	24. **Any "interference by a public authority" with the right to respect for correspondence will contravene Article 8 of the Convention unless it is "in accordance with the law", pursues one or more of the legitimate aims referred to in paragraph 2 of that Article and is "necessary in a democratic society" in order to achieve them (see,**

	correspondence; censorship; legal basis	**among many other authorities, Silver and Others v. the United Kingdom, 25 March 1983, Series A no. 61, p. 32, § 84; Campbell v. the United Kingdom, 25 March 1992, Series A no. 233, p. 16, § 34 and Niedbała v. Poland no. 27915/95, § 78).** 25. **As to the expression "in accordance with the law", the court has established three fundamental principles. The first one is that the interference in question must have some basis in domestic law. The second principle is that "the law must be adequately accessible"; a person must be able to have an indication that is adequate, in the circumstances, of the legal rules applicable to his case. The third principle is that "a norm cannot be regarded as a 'law' unless it is formulated with sufficient precision to enable a person to regulate his conduct; he must be able - if need be with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail" (see the Silver and Others v. the United Kingdom judgment cited above, §§ 86-88).** (b) Application of the above principles to the present case 28. The Court notes that the Government did not indicate a concrete legal basis for the impugned interference. The Court observes that the applicant in the present case served a sentence of imprisonment following his final conviction (see paragraph 10 above). In respect of convicted persons the domestic law provided a specific statutory prohibition on censorship of their correspondence with "institutions set up by international treaties ratified by the Republic of Poland concerning the protection of human rights." This prohibition was laid down in Article 103 § 1 of the 1997 Code (see paragraphs 13 above). That provision was expressed in plain terms and it did not leave a decision as to whether to censor the applicant's letter to the authorities' discretion but expressly forbade them from doing so (see G.K. v. Poland, no. 38816/97, § 110, 20 January 2004). **Since the authorities acted against that clear legal prohibition, the interference with the applicant's correspondence with the Court was not "in accordance with the law", as required by Article 8 of the Convention.** 29. Accordingly, there has been a breach of Article 8 in that respect. For that reason, the Court does not consider it necessary to examine the complaint that the facts of the case also give rise to an interference with the exercise of his right of individual petition pursuant to Article 34 of the Convention (see, Matwiejczuk v. Poland, cited above, § 103; and mutatis mutandis, Foxley v. the United Kingdom, no. 33274/96, § 47, 20 June 2000).
33.	Eur. Court HR, *Matheron v. France*, judgment of 29 March 2005, 57752/00: criminal proceedings; drug-trafficking; telephone tapping; effective control	**Judgment in French** From the Press Release: The applicant, Robert Matheron, is a French national who was born in 1949. He is currently in Salon de Provence Prison (France). In 1993 criminal proceedings were instituted against him for international drug-trafficking. Evidence obtained from telephone tapping that had been used in proceedings against a co-defendant was also used against the applicant. The applicant argued that that evidence was inadmissible, but the indictment division ruled that it had no jurisdiction to verify whether evidence obtained from telephone tapping in separate proceedings had been properly communicated and recorded in writing. On 6 October 1999 the Court of Cassation dismissed an appeal by the applicant, holding that the indictment division only had jurisdiction to determine the validity of

		the application to adduce the telephone records in evidence, but not to decide whether the telephone tapping was lawful. On 23 June 2000 the applicant was sentenced to 15 years' imprisonment. He complained under Article 8 of the Convention (right to respect for his private life) that evidence had been used against him that had been obtained from telephone tapping in separate proceedings. Not being a party to those proceedings, he had been unable to contest their validity. The main task of the Court was to ascertain whether an "effective control" had been available to the applicant to challenge the telephone tapping to which he had been made subject. It was clear that he had been unable to intervene in the proceedings in which the order to monitor telephone calls had been made. Furthermore, the Court of Cassation had ruled that in such cases the role of the indictment division was confined to checking whether the application to adduce evidence obtained from the telephone tapping had been made in the proper form. The Court reiterated that the 1991 Act regulating telephone tapping in France was consistent with the Convention. However, it said that the reasoning followed by the Court of Cassation could lead to decisions that would deprive a number of people, namely those against whom evidence obtained from telephone tapping in separate proceedings was used, of the protection afforded by the Act. That was what had happened in the case before the Court in which the applicant had not enjoyed the effective protection of the Act, which made no distinction on the basis of the proceedings in which the taped telephone conversations were used. In those circumstances, the Court found that the applicant had not had access to "effective control" allowing him to contest the validity of the evidence obtained through telephone tapping. It accordingly held unanimously that there had been a violation of Article 8 of the Convention and awarded the applicant EUR 3,500 for non-pecuniary damage and EUR 5,500 for costs and expenses. (The judgment is available only in French.) <u>Discussion of violation in §§ 27-44</u> B. Appréciation de la Cour 1. Existence d'une ingérence 27. La Cour souligne que les communications téléphoniques se trouvant comprises dans les notions de « vie privée » et de « correspondance » au sens de l'article 8, ladite interception s'analysait en une « ingérence d'une autorité publique » dans l'exercice d'un droit que le paragraphe 1 garantissait au requérant (voir notamment les arrêts Malone c. Royaume-Uni du 2 août 1984, série A no 82, p. 30, § 64, Kruslin c. France et Huvig c. France du 24 avril 1990, série A no 176-A et 176-B, p. 20, § 26, et p. 52, § 25, Halford c. Royaume-Uni du 25 juin 1997, Recueil 1997-III, pp. 1016-1017, § 48 ; Kopp c. Suisse du 25 mars 1998, Recueil 1998-II, p. 540, § 53 ; Lambert c. France du 24 août 1998, Recueil 1998-V, pp. 2238-2239, § 21). Le Gouvernement le reconnaît expressément. 2. Justification de l'ingérence 28. Pareille ingérence méconnaît l'article 8, sauf si « prévue par la loi », elle poursuit un ou des buts légitimes au regard du paragraphe 2 et, de plus, est « nécessaire dans une société démocratique » pour les atteindre. a) L'ingérence était-elle « prévue par la loi » ? 29. Les mots « prévue par la loi » au sens de l'article 8 § 2 veulent d'abord que la mesure incriminée ait une base en droit interne, mais ils ont trait aussi à la qualité de la loi en cause : ils exigent l'accessibilité de celle-ci à la

personne concernée, qui de surcroît doit pouvoir en prévoir les conséquences pour elle, et sa compatibilité avec la prééminence du droit.

30. La Cour rappelle que les interceptions des communications téléphoniques ordonnées par un juge d'instruction sur le fondement des articles 100 et suivants du code de procédure pénale ont une base légale en droit français (Lambert, précité, §§ 24-25).

31. Reste que si les articles 100 et suivants du code de procédure pénale réglementent l'emploi d'écoutes téléphoniques, sous certaines conditions, afin d'identifier les auteurs et les complices des faits sur lesquels porte l'instruction, il n'apparaît pas que la situation des personnes écoutées dans le cadre d'une procédure à laquelle elles sont étrangères soit couverte par ces dispositions. Or, en l'espèce, force est de constater que les écoutes litigieuses furent diligentées pour les seuls faits dont étaient saisis les juges d'instruction de Nancy et, partant, dans le cadre d'une procédure à laquelle M. Matheron était étranger.

32. La Cour pourrait être amenée à se poser la question de savoir si l'ingérence litigieuse était ou non « prévue par la loi » en l'espèce (voir, en particulier, Amann c. Suisse [GC], no 27798/95, CEDH 2000-II). Toutefois, elle n'estime pas devoir se prononcer sur ce point dès lors que la violation est encourue pour un autre motif.

b) Finalité et nécessité de l'ingérence

33. La Cour estime que l'ingérence visait à permettre la manifestation de la vérité dans le cadre d'une procédure criminelle et tendait donc à la défense de l'ordre.

34. Il reste à examiner si l'ingérence était « nécessaire dans une société démocratique » pour atteindre ces objectifs. Selon la jurisprudence constante de la Cour, les Etats contractants jouissent d'une certaine marge d'appréciation pour juger de l'existence et de l'étendue de pareille nécessité, mais elle va de pair avec un contrôle européen portant à la fois sur la loi et sur les décisions qui l'appliquent, même quand elles émanent d'une juridiction indépendante (voir, mutatis mutandis, les arrêts Silver et autres c. Royaume-Uni du 25 mars 1983, série A no 61, pp. 37–38, § 97 ; Barfod c. Danemark du 22 février 1989, série A no 149, p. 12, § 28 ; Lambert, précité, § 30).

35. Dans le cadre de l'examen de la nécessité de l'ingérence, la Cour avait affirmé, dans son arrêt Klass et autres c. Allemagne du 6 septembre 1978 (série A no 28, pp. 23 et 25, §§ 50, 54 et 55 ; voir également Lambert, précité, § 31) :
« Quel que soit le système de surveillance retenu, la Cour doit se convaincre de l'existence de garanties adéquates et suffisantes contre les abus. Cette appréciation ne revêt qu'un caractère relatif : elle dépend (...) [entre autres, du] type de recours fourni par le droit interne.

(...)

Par conséquent, il y a lieu de rechercher si les procédures destinées au contrôle de l'adoption et de l'application des mesures restrictives sont aptes à limiter à ce qui est « nécessaire dans une société démocratique » l'« ingérence » résultant de la législation incriminée.

(...) Il faut de surcroît, pour ne pas dépasser les bornes de la nécessité au sens de l'article 8 § 2, respecter aussi fidèlement que possible, dans les procédures de contrôle, les valeurs d'une société démocratique. Parmi les

principes fondamentaux de pareille société figure la prééminence du droit, à laquelle se réfère expressément le préambule de la Convention (...). Elle implique, entre autres, qu'une ingérence de l'exécutif dans les droits d'un individu soit soumise à un contrôle efficace (...) »

36. En l'espèce, la Cour doit donc rechercher si M. Matheron a disposé d'un « contrôle efficace » pour contester les écoutes téléphoniques dont il a fait l'objet.

37. Elle relève tout d'abord qu'il n'est pas contesté que le requérant ne pouvait en aucun cas intervenir dans le cadre de la procédure pénale diligentée à Nancy et dans le cadre de laquelle les écoutes téléphoniques avaient été ordonnées et effectuées. Partant, il convient d'examiner la procédure diligentée contre le requérant par un juge d'instruction de Marseille.

38. Or, dans son arrêt du 6 octobre 1999, la Cour de cassation a confirmé l'arrêt de la chambre d'accusation selon lequel, d'une part, en sollicitant régulièrement la communication des écoutes litigieuses et en ordonnant leur retranscription, le juge d'instruction n'a fait qu'user des prérogatives que lui confère l'article 81 du code de procédure pénale et, d'autre part, il n'appartient pas à la chambre d'accusation d'apprécier la régularité de décisions prises dans une procédure autre que celle dont elle est saisie, extérieure à son ressort, décisions par ailleurs insusceptibles de recours en application de l'article 100 du code précité.

39. En conséquence, pour la Cour de cassation, la chambre d'accusation devait se contenter, comme ce fut le cas, de contrôler la régularité de la demande de versement au dossier du requérant des pièces relatives aux écoutes, à l'exclusion de tout contrôle sur les écoutes elles-mêmes.

40. Certes, la Cour note, avec le Gouvernement, que les écoutes litigieuses avaient été ordonnées par un magistrat et réalisées sous son contrôle. Le Gouvernement considère que ce constat suffirait à établir l'existence d'un contrôle efficace et en déduit que l'appel devant la chambre d'accusation est inutile, se référant notamment à l'article 2 du Protocole no 7. La Cour ne partage pas cette analyse. En premier lieu, elle note que l'article 2 du Protocole no 7, qui n'a pas été invoqué par le requérant, est étranger aux faits de la cause. Par ailleurs, elle est d'avis qu'un tel raisonnement conduirait à considérer que la qualité de magistrat de celui qui ordonne et suit les écoutes impliquerait, ipso facto, la régularité des écoutes et leur conformité avec l'article 8, rendant inutile tout recours pour les intéressés.

41. Ainsi que la Cour l'a déjà jugé, les dispositions de la loi de 1991 régissant les écoutes téléphoniques répondent aux exigences de l'article 8 de la Convention et à celles des arrêts Kruslin et Huvig (Lambert, précité, § 28). Cependant, force est de constater que le raisonnement de la Cour de cassation pourrait conduire à des décisions privant de la protection de la loi un certain nombre de personnes, à savoir toutes celles qui se verraient opposer le résultat d'écoutes téléphoniques réalisées dans des procédures étrangères à la leur, ce qui reviendrait, en pratique, à vider le mécanisme protecteur d'une large partie de sa substance (ibidem, § 38).

42. Tel fut le cas pour le requérant qui n'a pas joui, en l'espèce, de la protection effective de la loi nationale, laquelle n'opère pas de distinction selon la procédure dans le cadre de laquelle les écoutes ont été ordonnées (paragraphe 17 ci-dessus ; voir, mutatis mutandis, ibidem, § 39).

43. Dès lors, la Cour estime que l'intéressé n'a pas bénéficié d'un «

		contrôle efficace » tel que voulu par la prééminence du droit et apte à limiter à ce qui était « nécessaire dans une société démocratique » l'ingérence litigieuse. 44. Partant, il y a eu violation de l'article 8 de la Convention.
34.	Eur. Court HR *Antunes Rocha v. Portugal*, judgment of 31 May 2005, 64330/01: security investigations; gatering of information; control mechanism; safeguards	**Judgment in French** <u>From the Press Release:</u> The Court found that the authorities' decision to gather information about the applicant constituted interference with her private life. On examining whether that interference was "in accordance with the law", as required by Article 8 § 2 of the Convention, the Court noted, firstly, that there was a legal basis for it in domestic law, namely Cabinet Resolution no. 50/88 of 8 September 1988, which was in fact still in force. The Court considered the aim of the legislation sufficiently clear, namely to establish whether the person concerned was totally honest and loyal and whether his or her reputation, habits, social life, discretion and commonsense were such as to permit him or her to be given access to confidential files. However, the same could not be said of the manner in which the inquiries had been conducted. The legislation was too vague and did not alert those concerned to the fact that they might be subject to certain measures, such as surveillance of their home or tests of knowledge. Furthermore, the legislation did not contain any control mechanisms or provide any safeguards for individuals. That too was unacceptable in the Court's view. Consequently, the Court found that Portuguese law did not indicate with sufficient clarity the scope of security investigations or the manner in which they were to be carried out. The gathering of the information about the applicant was not, therefore, "in accordance with the law". The Court accordingly held by seven votes to one that there had been a violation of Article 8 of the Convention. <u>Discussion of violation in §§ 62-80</u> B. Appréciation de la Cour 1. Sur l'existence d'une ingérence 62. La Cour relève d'abord que la collecte, la mémorisation et l'éventuelle communication de données relatives à la « vie privée » d'un individu entrent dans le champ d'application de l'article 8 § 1 de la Convention (Leander c. Suède, arrêt du 26 mars 1987, série A no 116, p. 22, § 48 ; Rotaru c. Roumanie [GC], no 28341/95, § 43, CEDH 2000-V). Même des données de nature publique peuvent relever de la vie privée lorsqu'elles sont, d'une manière systématique, recueillies et mémorisées dans des fichiers tenus par les pouvoirs publics (Rotaru précitée, ibidem). 63. Le Gouvernement indique qu'aucun élément relatif aux mesures d'enquête dénoncées par la requérante, notamment la surveillance de sa résidence et l'interrogation de ses connaissances, ne figure dans les archives de l'Autorité nationale de sécurité. 64. La Cour souligne de son côté que cette Autorité a affirmé que le dossier en cause était confidentiel. Si la Cour se doit de respecter les exigences de sécurité et de confidentialité formulées par le Gouvernement dans la mesure où elles sont raisonnables, ces exigences, en l'occurrence, empêchent de vérifier si les actes en question se sont effectivement produits. Aux yeux de la Cour, cependant, l'élément essentiel en l'espèce est que la requérante s'est plainte d'avoir fait l'objet de ces actes sans qu'il

lui ait été possible de prévoir cette éventualité au moment de signer les autorisations pertinentes.

65. La Cour admet donc qu'il y a eu une ingérence dans la « vie privée », au sens de l'article 8, de la requérante, ingérence causée par la collecte de renseignements effectuée à son sujet par les autorités, indépendamment de la question de savoir quelle forme a revêtu cette collecte. Que la requérante se soit ou non prêtée à une telle ingérence en signant les documents en cause – comme l'allègue le Gouvernement – est un point qui doit être traité dans le cadre de l'examen de la justification de l'ingérence, surtout s'agissant de savoir si cette dernière était « prévue par la loi ».

2. Justification de l'ingérence

66. La principale question qui se pose en l'espèce est en effet de savoir si l'ingérence peut se justifier au regard du paragraphe 2 de l'article 8. Ménageant une exception à un droit garanti par la Convention, ce paragraphe appelle une interprétation étroite. Si la Cour reconnaît que, dans une société démocratique, l'existence de services de renseignements peut s'avérer légitime, elle rappelle que le pouvoir de surveiller en secret les citoyens n'est tolérable d'après la Convention que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques. Pour ne pas enfreindre l'article 8, pareille ingérence doit avoir été « prévue par la loi », poursuivre un but légitime au regard du paragraphe 2 et, de surcroît, être nécessaire dans une société démocratique pour atteindre ce but (Rotaru précité, §§ 47 et 48).

67. L'expression « prévue par la loi » veut d'abord que l'ingérence ait une base en droit interne, mais l'observation de celui-ci ne suffit pas : la loi en cause doit être accessible à l'intéressé, qui en outre doit pouvoir en prévoir les conséquences pour lui (Malone c. Royaume-Uni, arrêt du 2 août 1984, série A no 82, pp. 31-32, § 66).

68. Dans le contexte particulier de contrôles secrets du personnel affecté à des secteurs touchant à la sécurité nationale, l'exigence de prévisibilité ne saurait cependant être la même qu'en maints autres domaines. La Cour a ainsi eu l'opportunité de préciser qu'une telle exigence ne saurait signifier qu'un individu doit se trouver en mesure d'escompter avec précision les vérifications auxquelles la police procédera à son sujet en s'efforçant de protéger la sécurité nationale. Néanmoins, dans un système applicable à tous les citoyens, la loi doit user de termes assez clairs pour leur indiquer de manière adéquate en quelles circonstances et sous quelles conditions elle habilite la puissance publique à se livrer à pareille ingérence secrète, et virtuellement dangereuse, dans leur vie privée (Leander précité, p. 23, § 51).

69. De même, pour s'assurer du respect du critère de la prévisibilité, il faut tenir compte aussi des instructions ou des pratiques administratives n'ayant pas force de loi, pour autant que les intéressés les connaissent suffisamment. Enfin, lorsque sa mise en œuvre s'opère au moyen de mesures secrètes, échappant au contrôle des personnes concernées comme du public, la loi elle-même, par opposition à la pratique administrative dont elle s'accompagne, doit définir l'étendue du pouvoir d'appréciation attribué à l'autorité compétente avec assez de netteté – compte tenu du but légitime poursuivi – pour fournir à l'individu une protection adéquate contre l'arbitraire (Leander précité, ibidem).

70. En l'espèce, l'ingérence en question avait une base légale en droit interne, à savoir la résolution du Conseil des Ministres no 50/88 du 8 septembre 1988, qui est d'ailleurs toujours en vigueur. Reste à savoir si

cette législation avait l'accessibilité et la prévisibilité voulues.

71. La Cour relève d'abord que la résolution no 50/88, publiée au Journal officiel, répondait sans nul doute à l'exigence d'accessibilité. Il s'agit donc essentiellement de rechercher si elle fixait avec une précision suffisante les conditions dans lesquelles les autorités compétentes pouvaient collecter et stocker des données à caractère personnel concernant la requérante.

72. Le Gouvernement répond par l'affirmative. Il considère que la requérante était en mesure de savoir, à la simple lecture des documents qui lui avaient été fournis, que des mesures d'enquête pourraient être prises en vue de son habilitation, et il ajoute qu'elle y a donné son consentement de manière libre et éclairée.

73. La requérante estime au contraire que, dans les documents ou la législation en cause, rien n'indiquait que l'enquête en question pourrait comporter des mesures de surveillance de sa maison ou l'interrogation de ses connaissances.

74. Se penchant sur les dispositions pertinentes, notamment celles de l'instruction no 4.2.4.2.1, la Cour ne trouve aucune définition, ne serait-ce qu'indicative, du type de mesures que peut impliquer une enquête de l'Autorité nationale de sécurité en vue de l'octroi d'une habilitation de sécurité. La résolution no 50/88 précise, il est vrai, que l'enquête doit permettre de déterminer si l'intéressé est d'une honnêteté et d'une loyauté à toute épreuve et si sa réputation, ses habitudes, sa vie sociale, sa discrétion et son bon sens autorisent à lui donner accès à des dossiers confidentiels. Le but de l'enquête est donc suffisamment précisé par la législation applicable. Cependant, en ce qui concerne les méthodes d'enquête, l'instruction no 4.2.4.2.1 se borne à indiquer qu'elles doivent se fonder sur « toute information disponible ». S'il est vrai que l'exigence de prévisibilité ne saurait signifier, dans ce domaine, que l'individu doit se trouver en mesure d'escompter avec précision toutes les mesures de vérification auxquelles la police ou les services compétents procéderont à son sujet (voir paragraphe 68 ci-dessus), la Cour ne peut accepter une indication aussi générale et vague que celle de la législation litigieuse. En effet, rien dans le texte de l'instruction ne laissait prévoir des mesures telles que la surveillance du domicile de l'intéressée ou l'interrogation de ses connaissances.

75. Rien de tel ne figure non plus dans les documents signés par la requérante lors de son recrutement. La Cour admet à cet égard que les documents en cause sont ceux qui ont été produits devant elle et devant les juridictions internes, les allégations de l'intéressée à ce sujet (voir paragraphe 57 ci-dessus) étant spéculatives et se trouvant infirmées par les conclusions du juge d'instruction, dans l'ordonnance de non-lieu du 25 février 2000 (voir paragraphe 29 ci-dessus). Néanmoins, il serait vain de chercher dans ces documents une quelconque indication qui eût laissé prévoir des mesures d'enquête telles que celles dénoncées par la requérante. Le premier de ces documents était en effet une fiche de renseignements factuels concernant les proches parents de l'intéressée (âge, adresse, profession, emplois occupés précédemment, séjours à l'étranger) et le second était une simple déclaration par laquelle la requérante s'engageait à respecter les règles de sécurité en vigueur à l'OTAN.

76. La Cour doit aussi se convaincre de l'existence de garanties adéquates et suffisantes contre les abus, car un système de surveillance secrète destiné à protéger la sécurité nationale comporte le risque de saper, voire

		de détruire, la démocratie au motif de la défendre (Klass et autres c. Allemagne, arrêt du 6 septembre 1978, série A no 28, pp. 23-24, §§ 49-50). En effet, pour que les systèmes de surveillance secrète soient compatibles avec l'article 8 de la Convention, ils doivent contenir des garanties établies par la loi et applicables au contrôle des activités des services concernés. Les procédures de contrôle doivent respecter aussi fidèlement que possible les valeurs d'une société démocratique, en particulier la prééminence du droit, à laquelle se réfère expressément le préambule de la Convention. Elle implique, entre autres, qu'une ingérence de l'exécutif dans les droits de l'individu soit soumise à un contrôle efficace (Rotaru précité, § 59). 77. En l'occurrence, la résolution no 50/88 ne contient aucun mécanisme de contrôle ni ne prévoit aucune garantie pour les particuliers. La Cour ne saurait non plus accepter un tel défaut. 78. La Cour souligne enfin que dans sa recommandation no 22/B/97 du 23 décembre 1997, le médiateur de Justice portugais attirait déjà l'attention des pouvoir exécutif et législatif sur les insuffisances de cette législation au regard de l'article 8 de la Convention ainsi que d'autres dispositions similaires de droit portugais et de droit international ; il affirmait que la personne concernée n'était pas en mesure de prévoir des ingérences graves dans sa vie privée et conseillait donc à l'administration de faire signer aux intéressés une déclaration écrite indiquant, de la manière la plus précise possible, les investigations dont ils pourraient faire l'objet aux fins de leur habilitation de sécurité (voir paragraphe 39 ci-dessus). Or rien ne semble avoir été fait par l'administration, malgré l'indication donnée par l'Autorité nationale de sécurité relativement à la mise à jour des instructions de sécurité en vigueur, laquelle mise à jour ne semble pas avoir eu lieu (voir paragraphe 35 ci-dessus). 79. La Cour en conclut que le droit interne n'indique pas avec assez de clarté l'étendue d'une enquête de sécurité et les modalités suivant lesquelles elle peut se dérouler. Ainsi, la collecte de données concernant la requérante n'était pas « prévue par la loi », ce qui suffit à constituer une méconnaissance de l'article 8 de la Convention. Cette circonstance dispense la Cour d'examiner de surcroît si la collecte en question visait un but légitime et si elle était « nécessaire dans une société démocratique». 80. Partant, il y a eu violation de l'article 8.
35.	Eur. Court HR, *Vetter v. France*, judgment of 31 May 2005, 59842/00: police use of covert listening devices; inadequate specificity of law; *ultra vires* action by police	**Judgment in French** <u>From the legal summary:</u> The point in issue was whether the use of listening devices was "in accordance with the law". The bugging of private premises was manifestly not within the scope of Articles 100 et seq. of the Code of Criminal Procedure, since those provisions concerned the interception of telephone lines. Article 81 of the Code did not indicate with reasonable clarity the scope and manner of exercise of the authorities' discretion in allowing the monitoring of private conversations (see *Kruslin* and *Huvig v. France*, judgments of 24 April 1990) and the respondent Government had not claimed that that shortcoming had been adequately remedied by the relevant case-law. Accordingly, the applicant had not enjoyed the minimum degree of protection to which citizens were entitled under the rule of law in a democratic society. *Conclusion:* violation (unanimously). <u>Discussion of violation of Article 8 in §§ 20-29</u> 20. La Cour souligne que les faits dénoncés par le requérant caractérisent

sans aucun doute une ingérence dans les droits garantis par l'article 8 § 1 de la Convention, d'autant plus que l'opération de « sonorisation » en cause visait clairement l'interception des propos de l'intéressé. Elle renvoie à cet égard à son arrêt *Khan c. Royaume-Uni* du 12 mai 2000 (no 35394/97, CEDH 2000-V, § 26), relatif à des circonstances similaires.
Il reste à déterminer si cette ingérence se justifiait au regard du second paragraphe de l'article 8, c'est-à-dire si elle était « prévue par la loi », inspirée par l'un ou plusieurs des buts légitimes qu'il énonce et était « nécessaire » « dans une société démocratique » pour les atteindre.

21. Sur le premier point, la Cour rappelle que les mots « prévue par la loi », au sens de l'article 8 § 2, veulent d'abord que la mesure incriminée ait une base en droit interne ; pour juger de l'existence d'une telle « base légale », il y a lieu de prendre en compte non seulement les textes législatifs pertinents, mais aussi la jurisprudence (voir, par exemple, l'arrêt *Kruslin* précité, §§ 27 et 29).

22. En l'espèce, les juridictions internes ont conclu que l'ingérence litigieuse trouvait sa base légale dans les articles 81 et 100 et suivants du code de procédure pénale.

23. La Cour relève tout d'abord que les articles 100 et suivants du code de procédure pénale – insérés dans ce code par la loi no 91-646 du 10 juillet 1991 sur le secret des correspondances émises par la voie des communications électroniques – ne contiennent aucune référence à la « sonorisation », que leur texte, ainsi que le titre qui les précède, indiquent qu'ils se bornent à régir les « interceptions de correspondances émises par la voie des télécommunications », et que la circulaire générale du 26 septembre 1991 (article C. 100) précise à cet égard qu'entrent « dans le champ d'application de [l'article 100], les interceptions de correspondances émises ou reçues sur des équipements terminaux tels que téléphone, télécopieur, minitel, récepteurs de services de radiomessagerie unilatérale, télex » (paragraphe 15 ci-dessus). Il est donc surprenant qu'en l'espèce, dans son arrêt du 15 février 2000, la chambre criminelle de la Cour de cassation conclue que la « sonorisation » d'un appartement puisse trouver son fondement légal dans ces dispositions. La Cour note ensuite que cet arrêt n'a pas de précédent.
La Cour n'est donc pas convaincue que, lorsqu'elle a été ordonnée puis mise en oeuvre, la « sonorisation » litigieuse trouvait une base légale dans les articles 100 et suivants du code de procédure pénale ; au demeurant, le Gouvernement ne défend pas une telle thèse.

24. Quant à l'article 81 du code de procédure pénal, il dispose que « le juge d'instruction procède, conformément à la loi, à tous les actes d'information qu'il juge utiles à la manifestation de la vérité » ; il précise que le magistrat peut donner commission rogatoire à cette fin dans les conditions et sous les réserves prévues aux articles 151 et 152.
La Cour n'a cependant identifié aucun arrêt de cassation antérieur aux circonstances de la cause, dont il ressortirait que cette disposition constitue une base légale suffisante à la « sonorisation », en tant que telle, d'un appartement sur commission rogatoire. Quant à l'arrêt de la chambre criminelle de la Cour de cassation du 23 novembre 1999 (pourvoi no 99-82658) auquel se réfère le Gouvernement, il se borne à conclure que « le juge d'instruction tient des articles 81, alinéa premier, 151 et 152 du code de procédure pénale le pouvoir de prescrire, en vue de la constatation des infractions, tous les actes d'information utiles à la manifestation de la vérité, y compris l'enregistrement de conversations privées, pourvu que (...) ces mesures aient lieu sous son contrôle et dans des conditions ne portant pas atteinte aux droits de la défense ». Il semble en vérité que la jurisprudence antérieure aux faits de la cause allait dans le sens contraire

(voir l'arrêt de la chambre criminelle de la Cour de Cassation du 16 décembre 1997 sur le pourvoi no96-85589 ; paragraphe 16 ci-dessus).

25. A supposer qu'il puisse néanmoins être considéré que la mesure litigieuse trouve son fondement légal dans les articles 81, 151 et 152 du code de procédure pénal, la Cour estime que la « loi » ainsi identifiée ne remplit pas les conditions qualitatives consacrées par sa jurisprudence.

26. La Cour rappelle à cet égard que la « loi » doit notamment être « prévisible » « quant au sens et à la nature des mesures applicables » : elle doit être « compatible avec la prééminence du droit », et « offrir une certaine protection contre des atteintes arbitraires de la puissance publique aux droits garantis par le paragraphe 1 [de l'article 8] » (arrêt*Kruslin* précité, § 30). En outre, la « loi » doit user de termes assez clairs pour indiquer aux individus de manière suffisante en quelles circonstances et sous quelles conditions elle habilite les autorités publiques à prendre des mesures de surveillance secrète (voir les arrêts *Malone c. Royaume-Uni*, du 2 août 1984, série A no 82, § 67, et *Khan*, précité, § 26).
La Cour estime que, comme les interceptions d'entretiens téléphoniques, les écoutes de conversations par le biais de la pose de micros représentent une atteinte grave au respect de la vie privée. Elles doivent donc se fonder sur une « loi » d'une précision particulière : dans ce domaine aussi, l'existence de règles claires et détaillées apparaît indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner (voir, notamment, l'arrêt *Kruslin* précité, §§ 32 et 33). Selon la Cour, la « loi » doit offrir aux justiciables « des sauvegardes adéquates » contre les abus à redouter (arrêt *Kruslin* précité, § 35), de même nature qu'en matière d'écoutes téléphoniques. Ainsi, notamment, les catégories de personnes susceptibles de faire l'objet d'une telle mesure et la nature des infractions pouvant y donner lieu doivent être définies ; le juge doit être astreint à fixer une limite à la durée de l'exécution de la mesure ; doivent également être précisées les conditions d'établissement des procès-verbaux de synthèse consignant les conversations « écoutées », les précautions à prendre pour communiquer intacts et complets les enregistrements réalisés, aux fins de contrôle éventuel par le juge et par la défense, ainsi que les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction desdites bandes, notamment après non-lieu ou relaxe (*ibidem*, ainsi que le paragraphe 34). Or, d'une part, les articles 81, 151 et 152 du code de procédure pénale ne contiennent pas de dispositions de cette nature et, d'autre part, le Gouvernement ne prétend pas que cette lacune se trouve adéquatement comblée par la jurisprudence.

27. Bref, renvoyant à son raisonnement dans les arrêts *Kruslin c. France* (précité) et *Huvig c. France* (mêmes références) – qui concernent l'organisation des écoutes téléphoniques en France avant l'entrée en vigueur de la loi no 91-646 du 10 juillet 1991 sur le secret des correspondances émises par la voie des communications électroniques – la Cour ne peut que constater que, dans le domaine de la pose de micros, le droit français n'indique pas avec assez de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités. Relevant au surplus que le Gouvernement admet que « cette jurisprudence paraît, *mutatis mutandis*, applicable à la présente espèce » et déclare en conséquence « s'en remet[tre] à la sagesse de la Cour quant au grief tiré de l'article 8 en matière de sonorisation », la Cour conclut que le requérant n'a pas joui du degré minimal de protection voulu par la prééminence du droit dans une société démocratique et qu'il y a eu violation de l'article 8 de la Convention.

28. La Cour rappelle que l'affaire *Lambert* citée par les parties concernait

		l'écoute et l'interception de conversations téléphoniques du requérant, sur le fondement de la loi no91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques ; l'intéressé se plaignait devant elle du fait qu'il s'était vu refuser toute qualité pour invoquer la protection de la loi nationale ou celle de l'article 8 de la Convention devant les juridictions internes, au motif que la ligne sous écoute était celle d'un tiers. La Cour a estimé que les dispositions de la loi du 10 juillet 1991 « répond[ai]ent aux exigences de l'article 8 de la Convention et à celles des arrêts *Kruslin* et*Huvig* » (paragraphe 38 de l'arrêt ; voir aussi le paragraphe 28). Ainsi, elle n'a pas jugé que l'ingérence critiquée n'était pas « prévue par la loi » ; la conclusion de violation de l'article 8 auquel elle est parvenue repose sur le constat que M. Lambert n'avait pas bénéficié d'un « contrôle efficace » des écoutes téléphoniques dont il avait fait l'objet en application de la loi de 1991, tel que voulu par la prééminence du droit, et apte à limiter cette ingérence à ce qui était « nécessaire dans une société démocratique » au sens de l'article 8 § 2 (paragraphe 40 de l'arrêt). Ainsi, si la présente espèce se rapproche de l'affaire *Lambert* en ce que, parce que la sonorisation litigieuse avait été effectuée dans l'appartement d'un tiers, la chambre criminelle de la Cour de cassation a jugé dans son arrêt du 15 février 2000 que le requérant ne pouvait se dire personnellement victime d'une violation des règles de procédures portant atteinte à l'intimité de la vie privée et, en conséquence, n'avait pas qualité pour invoquer une telle violation, elle s'en distingue substantiellement en ce que la Cour a conclu à une violation de l'article 8 au motif que l'ingérence dans le droit du requérant au respect de sa vie privée n'était pas « prévue par la loi » au sens du second paragraphe de cette disposition (paragraphes 26-27 ci-dessus) ; dans de telles circonstances, il n'y a pas lieu de rechercher si elle visait un « but légitime » et si elle était « nécessaire dans une société démocratique » au sens de ce même paragraphe (voir, par exemple, les arrêts *Huvig* et *Khan* précités, § 37 et § 28 respectivement). 29. La Cour estime par ailleurs qu'aucune question distincte ne se pose en l'espèce sur le terrain de l'article 6 de la Convention du fait du rejet par la chambre criminelle de la Cour de cassation, pour « défaut de qualité à agir », du moyen du requérant fondé sur l'article 8 de la Convention.
36.	Eur. Court HR, *Wisse v. France*, judgment of 20 December 2005, 71611/01: law enforcement surveillance of conversations in prison visiting room; conversations in prison visiting rooms within scope of Article 8; Insufficient precision in law regarding surveillance of conversations in this sphere	**Judgment in French** <u>From the Press Release:</u> In the Court's view, the systematic recording of conversations in a visiting room for purposes other than prison security deprived visiting rooms of their sole *raison d'être*, namely to allow detainees to maintain some degree of "private life", including the privacy of conversations with their families. The conversations conducted in a prison visiting room, therefore, could be regarded as falling within the scope of the concepts of "private life" and "correspondence". <u>Discussion of violation in §§ 24-34</u> 24. La Cour a rappelé maintes fois que la vie privée est une notion large qui ne se prête pas à une définition exhaustive. Des facteurs tels que l'identification sexuelle, le nom, l'orientation sexuelle et la vie sexuelle sont des éléments importants de la sphère personnelle protégée par l'article 8. Cette disposition protège également le droit à l'identité et au développement personnel, ainsi que le droit pour tout individu de nouer et développer des relations avec ses semblables et le monde extérieur. Il peut s'étendre à des activités professionnelles ou commerciales. Il existe donc une zone d'interaction entre l'individu et autrui qui, même dans un

contexte public, peut relever de la « vie privée » (*Peck c. Royaume-Uni*, no 44647/98, § 57, ECHR 2003-I).

25. Elle a précisé également ce qui suit :
« Un certain nombre d'éléments entrent en ligne de compte lorsqu'il s'agit de déterminer si la vie privée d'une personne est touchée par des mesures prises en dehors de son domicile ou de ses locaux privés. Puisqu'à certaines occasions les gens se livrent sciemment ou intentionnellement à des activités qui sont ou peuvent être enregistrées ou rapportées publiquement, ce qu'un individu est raisonnablement en droit d'attendre quant au respect de sa vie privée peut constituer un facteur significatif, quoique pas nécessairement décisif. Une personne marchant dans la rue sera forcément vue par toute autre personne qui s'y trouve aussi. Le fait d'observer cette scène publique par des moyens techniques (par exemple un agent de sécurité exerçant une surveillance au moyen d'un système de télévision en circuit fermé) revêt un caractère similaire. En revanche, la création d'un enregistrement systématique ou permanent de tels éléments appartenant au domaine public peut donner lieu à des considérations liées à la vie privée » (*P.G. et J.H. c. Royaume-Uni,* no 44787/98, § 56, CEDH 2001-IX).

26. La Cour a ainsi distingué la surveillance des actes d'un individu dans un lieu public à des fins de sécurité des enregistrements de ces actes qui seraient utilisés à d'autres fins allant au delà de ce que l'intéressé aurait pu prévoir (*Peck* précité, §§ 59 à 62, et *Perry c. Royaume-Uni*, no 63737/00, 17 juillet 2003, §§ 41 et 42) pour établir, dans le domaine des mesures secrètes de surveillance ou de l'interception de communication par les autorités publiques, la frontière de l'intimité de la vie privée garantie par l'article 8 de la Convention.

27. Dans sa jurisprudence, elle a souvent constaté que l'interception secrète de conversations ou d'images par le biais d'appareils d'enregistrement audio et vidéo entrait dans le champ d'application de l'article 8 de la Convention pour ce qui est tant du droit au respect de la vie privée que de la correspondance. Elle l'a fait, par exemple, quant à l'enregistrement secret de conversations au moyen d'un système d'écoute par la police dans l'appartement d'une personne soupçonnée de se livrer à un trafic de stupéfiants (*Khan c. Royaume-Uni*, no35394/97, § 25, ECHR 2000-V ; voir également, sur la sonorisation de l'appartement d'un individu où la police savait qu'un autre devait se rendre dans le cadre d'une information judiciaire pour homicide, *Vetter c. France*, no59842/00, 31 mai 2005, § 26). Elle a appliqué cette jurisprudence dans le cas de personnes surveillées alors qu'elles étaient dans des lieux de détention. Elle l'a ainsi fait, par exemple, en cas d'utilisation d'appareils d'écoutes dans une cellule d'un commissariat de police (*P.G. et J.H.* précité), de réalisation d'un film dans la salle de garde à vue d'un tel commissariat (*Perry* précité), de la mise en place d'un dispositif de surveillance audio et vidéo placé dans la cellule d'un détenu en prison et dans la zone de visite de celle-ci (*Allan* précité), de l'enregistrement et de la conservation de conversations téléphoniques d'un prisonnier par les autorités pénitentiaires, ensuite utilisés comme élément de preuve pour le condamner pour une autre infraction (*Doerga c. Pays-Bas*, no 50210/99, 27 avril 2004), et d'un placement d'un détenu sous surveillance vidéo permanente pour une période de deux semaines (*Van der Graaf c. Pays-Bas* (déc), no 8704/03, 1er juin 2004).

28. En l'espèce, les juridictions nationales considèrent que dès lors que les propos tenus dans les parloirs sont en tout état de cause soumis à surveillance, c'est en connaissance de cause que les accusés et leurs visiteurs les échangent sans qu'il y ait ingérence de ce fait dans leur vie

privée. Le Gouvernement approuve ce raisonnement.

29. La Cour ne partage pas ce point de vue. Si l'écoute par l'administration pénitentiaire des conversations tenues au parloir est effectuée dans un souci de sécurité de la détention, parfaitement légitime, l'enregistrement systématique de celles-ci à d'autres fins dénie à la fonction du parloir sa seule raison d'être, celle de maintenir une « vie privée » du détenu - relative - qui englobe l'intimité des propos tenus avec ses proches. Les conversations tenues dans le parloir d'une prison peuvent en conséquence se trouver comprises dans les notions de « vie privée » et de « correspondance ».

30. Dès lors que l'article 8 s'applique au grief des requérants, la Cour n'aperçoit pas de raisons de s'écarter de sa jurisprudence en la matière (paragraphe 27 ci-dessus) pour conclure à l'existence d'une ingérence dans le cas présent. La ruse employée par la police sur commission rogatoire du juge d'instruction pour obtenir des informations sur la recherche de la vérité va nettement au-delà des mesures de surveillance du parloir telles que prévues par l'article D. 406 du CPP, excédant en tout cas ce qui peut être contrôlé à des fins de sécurité. En outre, les requérants, placés en détention provisoire, et recevant les premières visites de leurs compagnes, pouvaient espérer une certaine intimité, ce qui implique un certain degré de liberté dans la conversation. Rien n'indique qu'ils se soient attendus à ce que leurs conversations soient enregistrées au parloir dans le dessein de constituer des preuves susceptibles d'être produites au cours du procès. Dans ces conditions, la Cour considère que l'enregistrement et l'utilisation subséquente des conversations tenues au parloir par les requérants avec leurs proches s'analysent en une ingérence dans leur vie privée, si bien que l'exception du Gouvernement qu'elle a jointe au fond (voir § 17 ci-dessus) ne peut qu'être écartée.

31. Il lui reste à déterminer si cette ingérence se justifiait au regard du second paragraphe de l'article 8, c'est-à-dire si elle était « prévue par la loi », inspirée par l'un ou plusieurs des buts légitimes qu'il énonce et était « nécessaire » « dans une société démocratique » pour les atteindre.

32. Sur le premier point, la Cour rappelle que les mots « prévue par la loi », au sens de l'article 8 § 2, veulent d'abord que la mesure incriminée ait une base en droit interne ; pour juger de l'existence d'une telle « base légale » il y a lieu de prendre en compte non seulement les textes législatifs pertinents, mais aussi la jurisprudence (voir, par exemple, les arrêts *Kruslin c. France* et *Huvig c. France* du 24 avril 1990 (série A nos 176-A et 176-B).

33. En l'espèce, les juridictions internes ont conclu que l'ingérence litigieuse trouvait sa base légale dans les articles 81, 151 et 152 du CPP. A supposer que le seul arrêt de la cour de cassation cité par le Gouvernement, et antérieur à celui de la présente affaire, puisse constituer une base légale à l'enregistrement des conversations dans les parloirs des prisons, la Cour rappelle que, à l'instar des interceptions d'entretiens téléphoniques[1] ou des écoutes de conversations par le biais de la pose de micros[2], la loi sur laquelle il se fonde doit être « prévisible » quant au sens et à la nature des mesures applicables. La Cour a constamment rappelé que les conditions qualitatives comprises dans les mots « prévues par la loi » au sens de l'article 8 § 2 exigent l'accessibilité de la loi à la personne concernée, qui de surcroît doit pouvoir en prévoir les conséquences pour elle, et sa compatibilité avec la prééminence du droit (*Matheron c. France*, no 57752/00,
29 mars 2005, § 29). Parmi les « sauvegardes adéquates » contre les abus à redouter figurent les catégories de personnes susceptibles de faire

		l'objet d'une telle mesure et la nature des infractions pouvant y donner lieu doivent être définies ; le juge doit être astreint à fixer une limite à la durée de l'exécution de la mesure ; doivent également être précisées les conditions d'établissement des procès-verbaux de synthèse consignant les conversations « écoutées », les précautions à prendre pour communiquer intacts et complets les enregistrements réalisés, aux fins de contrôle éventuel par le juge et par la défense, ainsi que les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction desdites bandes, notamment après non-lieu ou relaxe (*Kruslin* précité, § 34). Or, d'une part, les articles 81, 151 et 152 du C.P.P ne contiennent pas de dispositions de cette nature et, d'autre part, cette lacune n'est pas adéquatement comblée par la jurisprudence (paragraphe 23 ci-dessus). 34. La Cour considère dès lors que dans le domaine des enregistrements des conversations tenues dans les parloirs des prisons, le droit français n'indique pas avec assez de clarté la possibilité d'ingérence par les autorités dans la vie privée des détenus, ainsi que l'étendue et les modalités d'exercice de leur pouvoir d'appréciation dans ce domaine. Elle conclut que les requérants n'ont pas joui du degré minimal de protection voulu par la prééminence du droit dans une société démocratique et qu'il y a eu violation de l'article 8 de la Convention, sans qu'il soit besoin de trancher les autres conditions posées par l'article 8, à savoir que l'ingérence doit viser un but légitime et être nécessaire, dans une société démocratique.
37.	Eur. Court HR, *Turek v. Slovakia*, judgment of 14 February 2006, 57986/00: access to secret services documentations in lustration; Court recognizes tlegitimate ground to limit access to documents in secret service archives; secret rules regarding access to documents place an unfair burden on claimant; secret rules of access do not respect the principle of equality	115. **The Court recognises that, particularly in proceedings related to the operations of state security agencies, there may be legitimate grounds to limit access to certain documents and other materials.** However, in respect of lustration proceedings, this consideration loses much of its validity. In the first place, lustration proceedings are, by their very nature, oriented towards the establishment of facts dating back to the communist era and are not directly linked to the current functions and operations of the security services. Thus, unless the contrary is shown on the facts of a specific case, it cannot be assumed that there remains a continuing and actual public interest in imposing limitations on access to materials classified as confidential under former regimes. **Secondly, lustration proceedings inevitably depend on the examination of documents relating to the operations of the former communist security agencies. If the party to whom the classified materials relate is denied access to all or most of the materials in question, his or her possibilities to contradict the security agency's version of the facts would be severely curtailed.** Finally, under the relevant laws, it is typically the security agency itself that has the power to decide what materials should remain classified and for how long. **Since, it is the legality of the agency's actions which is in question in lustration proceedings, the existence of this power is not consistent with the fairness of the proceedings, including the principle of equality of arms. Thus, if a State is to adopt lustration measures, it must ensure that the persons affected thereby enjoy all procedural guarantees under the Convention in respect of any proceedings relating to the application of such measures.** 116. In the present case the applicant was asserting his rights in the context of an interference with them which had been occasioned by State power and arguably without his knowledge. **The courts considered it crucial for the applicant to prove that the interference was contrary to the applicable rules. These rules were, however, secret and the applicant did not have full access to them. On the other hand, the State – in the person of the SIS – did have full access. In those circumstances, and irrespectively of whether the placing of the**

		burden of proof on the applicant was compatible with domestic law, that requirement placed an unrealistic burden on him in practice and did not respect the principle of equality. It was thus excessive. The applicant's proceedings therefore cannot be considered as offering him effective protection of his right to respect for his private life. The Court arrives at this conclusion without embarking on an examination of the assessment of evidence in this case, which, in its view, is also open to criticism.
38.	Eur. Court HR, *Segerstedt-Wiberg and Others v. Sweden* judgment of 6 June 2006, 62332/00: applicants attempt to view secret services files on them; legitimate existence of secret services in a democratic society; age of information significant in justifying retention; contents of party manifesto cannot be taken alone in determining party objectives; refusal of access to files only legitimate where access would harm state interests	88. **While the Court recognises that intelligence services may legitimately exist in a democratic society, it reiterates that powers of secret surveillance of citizens are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions (see *Klass and Others v. Germany*, 6 September 1978, § 42, Series A no. 28, and *Rotaru*, cited above, § 47). Such interference must be supported by relevant and sufficient reasons and must be proportionate to the legitimate aim or aims pursued. In this connection, the Court considers that the national authorities enjoy a margin of appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved.** In the instant case, the interest of the respondent State in protecting its national security and combating terrorism must be balanced against the seriousness of the interference with the respective applicants' right to respect for private life. Here again the Court will limit its examination to the period from 1999 onwards. 90. **However, as to the information released to the second applicant (namely, his participation in a political meeting in Warsaw in 1967), the Court, bearing in mind the nature and age of the information, does not find that its continued storage is supported by reasons which are relevant and sufficient as regards the protection of national security.** **Similarly, the storage of the information released to the fifth applicant could for the most part hardly be deemed to correspond to any actual relevant national security interests for the respondent State. The continued storage of the information to the effect that he, in 1969, had allegedly advocated violent resistance to police control during demonstrations was supported by reasons that, although relevant, could not be deemed sufficient thirty years later.** 91. **However, the Court reiterates that "the constitution and programme of a political party cannot be taken into account as the sole criterion for determining its objectives and intentions; the contents of the programme must be compared with the actions of the party's leaders and the positions they defend" (see, *mutatis mutandis*, *Refah Partisi (the Welfare Party) and Others v. Turkey* [GC], nos. 41340/98, 41342/98, 41343/98 and 41344/98, § 101, ECHR 2003-II; *United Communist Party of Turkey and Others v. Turkey*, 30 January 1998, § 46, *Reports* 1998-I; *Socialist Party and Others v. Turkey*, 25 May 1998, § 50, *Reports* 1998-III; and *Freedom and Democracy Party (ÖZDEP) v. Turkey* [GC], no.23885/94, § 45, ECHR 1999-VIII).** This approach, which the Court has adopted in assessing the necessity under Article 11 § 2 of the Convention of the dissolution of a political party, is also pertinent for assessing the necessity in the interests of national security under Article 8 § 2 of collecting and storing information on a secret police register about the leaders and members of a political party. In this case, the KPML(r) party programme was the only evidence relied on by the Government. Beyond that, they did not point to any specific circumstance indicating that the impugned programme clauses were

		reflected in actions or statements by the party's leaders or members and constituted an actual or even potential threat to national security when the information was released in 1999, almost thirty years after the party had come into existence. Therefore, the reasons for the continued storage of the information about the third and fourth applicants, although relevant, may not be considered sufficient for the purposes of the necessity test to be applied under Article 8 § 2 of the Convention. Thus, the continued storage of the information released to the respective applicants in 1999 amounted to a disproportionate interference with their right to respect for private life. 102. **The Court notes that, according to the Convention case-law, a refusal of full access to a national secret police register is necessary where the State may legitimately fear that the provision of such information may jeopardise the efficacy of a secret surveillance system designed to protect national security and to combat terrorism (see *Klass andOthers*, cited above, § 58, and *Leander*, cited above, § 66).** In this case the national administrative and judicial authorities involved all held that full access would jeopardise the purpose of the system. The Court does not find any ground on which it could arrive at a different conclusion
39.	Eur. Court HR, *Liberty and others v. United Kingdom*, 58243/00: secret services monitoring of NGO communications; existence of legislatoion allowing monitoring constitutes an interference with Article 8; domestic legislation intransparent regaring surveillance	67.The fact that the Commissioner in his annual reports concluded that the Secretary of State's "arrangements" had been complied with (see paragraphs 32-33 above), while an important safeguard against abuse of power, did not contribute towards the accessibility and clarity of the scheme, since he was not able to reveal what the "arrangements" were. **In this connection the Court recalls its above case-law to the effect that the procedures to be followed for examining, using and storing intercepted material, *inter alia*, should be set out in a form which is open to public scrutiny and knowledge.** 68. **The Court notes the Government's concern that the publication of information regarding the arrangements made by the Secretary of State for the examination, use, storage, communication and destruction of intercepted material during the period in question might have damaged the efficacy of the intelligence-gathering system or given rise to a security risk. However, it observes that the German authorities considered it safe to include in the G10 Act, as examined in *Weber and Saravia* (cited above), express provisions about the treatment of material derived from strategic interception as applied to non-German telephone connections. In particular, the G10 Act stated that the Federal Intelligence Service was authorised to carry out monitoring of communications only with the aid of search terms which served, and were suitable for, the investigation of the dangers described in the monitoring order and which search terms had to be listed in the monitoring order (op. cit., § 32). Moreover, the rules on storing and destroying data obtained through strategic monitoring were set out in detail in section 3(6) and (7) and section 7(4) of the amended G10 Act (see *Weber and Saravia,* cited above, § 100). The authorities storing the data had to verify every six months whether those data were still necessary to achieve the purposes for which they had been obtained by or transmitted to them. If that was not the case, they had to be destroyed and deleted from the files or, at the very least, access to them had to be blocked; the destruction had to be recorded in minutes and, in the cases envisaged in section 3(6) and section 7(4), had to be supervised by a staff member qualified to hold judicial office. The G10 Act further set out detailed provisions governing the transmission, retention and use of data obtained through the interception of external communications (op. cit., §§ 33-**

		50). In the United Kingdom, extensive extracts from the Code of Practice issued under section 71 of the 2000 Act are now in the public domain (see paragraph 40 above), which suggests that it is possible for a State to make public certain details about the operation of a scheme of external surveillance without compromising national security.
40.	Eur. Court HR, *Cemalettin Canlı v. Turkey*, judgment of 18 November April 2008, 22427/04: police provide incomplete file to prosecutor; public information in scope of Article 8 where systematically collected and stored by authorities; right to reputation part of private life; retaining and using inaccurate files constitutes a violation.	33. The first issue for the Court to deal with is whether the information in the police report constituted data pertaining to the applicant's "private life" or whether it was "public information" and therefore not within the scope of Article 8 of the Convention. **The Court has had regard to the scope of the notion of "private life" as interpreted in its case-law (see, in particular, *Amann v. Switzerland* [GC], no. 27798/95, § 65 ECHR 2000-II, and *Rotaru v. Romania* [GC], no. 28341/95, § 43, ECHR 2000-V) from which it appears that "public information" can fall within the scope of "private life" where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past, as in the present case (*Rotaru*, § 43).** 34. The Court considers this interpretation of the notion of "private life" to be in line with the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985 and whose purpose is "to secure ... for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy with regard to automatic processing of personal data relating to him" (Article 1), such personal data being defined in Article 2 as "any information relating to an identified or identifiable individual" (paragraph 17 above). **42. Nevertheless, as pointed out above, not only was the information set out in the report false, but it also omitted any mention of the applicant's acquittal and the discontinuation of the criminal proceedings. Moreover, the decisions rendered in 1990 were not appended to the report when it was submitted to the Ankara court in 2003. These failures, in the opinion of the Court, were contrary to the unambiguous requirements of the Police Regulations and removed a number of substantial procedural safeguards provided by domestic law for the protection of the applicant's rights under Article 8 of the Convention (see, *mutatis mutandis*, *Craxi v. Italy (no. 2)*, no. 25337/94, § 82, 17 July 2003).**
41.	Eur. Court HR, *K.U. v. Finland*, judgment of 2 December 2008, 2872/02: anonymous posting of minor's information on dating site; service provider refuses to provide police with name of posting party; age of applicant significant; insufficient remedy in domestic law	48. **The Court accepts that, in view of the difficulties involved in policing modern societies, a positive obligation must be interpreted in a way which does not impose an impossible or disproportionate burden on the authorities or, as in this case, the legislator. Another relevant consideration is the need to ensure that powers to control, prevent and investigate crime are exercised in a manner which fully respects the due process and other guarantees which legitimately place restraints on criminal investigations and bringing offenders to justice, including the guarantees contained in Articles 8 and 10 of the Convention, guarantees which offenders themselves can rely on. The Court is sensitive to the Government's argument that any legislative shortcoming should be seen in its social context at the time. The Court notes at the same time that the relevant incident took place in 1999, that is, at a time when it was well-known that the Internet, precisely because of its anonymous character, could be used for criminal purposes (see paragraphs 22 and 24 above). Also, the widespread problem of child sexual abuse had become well known over the preceding decade. Therefore, it cannot be said that the**

		respondent Government did not have the opportunity to put in place a system to protect child victims from being exposed as targets for paedophiliac approaches via the Internet. **49. The Court considers that practical and effective protection of the applicant required that effective steps be taken to identify and prosecute the perpetrator, that is, the person who placed the advertisement. In the instant case, such protection was not afforded. An effective investigation could never be launched because of an overriding requirement of confidentiality. Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others. Without prejudice to the question whether the conduct of the person who placed the offending advertisement on the Internet can attract the protection of Articles 8 and 10, having regard to its reprehensible nature, it is nonetheless the task of the legislator to provide the framework for reconciling the various claims which compete for protection in this context. Such framework was not, however, in place at the material time, with the result that Finland's positive obligation with respect to the applicant could not be discharged. This deficiency was later addressed. However, the mechanisms introduced by the Exercise of Freedom of Expression in Mass Media Act (see paragraph 21 above) came too late for the applicant.**
42.	Eur. Court HR, *S. and Marper v. the United Kingdom*, judgment of 4 December 2008, 30562/04 and 30566/04: police retention of fingerprints and DNA; retention of DNA and fingerprints an interference with Artile 8; indefinite retention regardless of gravity of offence or conviction disproportionate	68. **The Court notes at the outset that all three categories of the personal information retained by the authorities in the present case, namely fingerprints, DNA profiles and cellular samples, constitute personal data within the meaning of the Data Protection Convention as they relate to identified or identifiable individuals. The Government accepted that all three categories are "personal data" within the meaning of the Data Protection Act 1998 in the hands of those who are able to identify the individual.** 71. **The Court maintains its view that an individual's concern about the possible future use of private information retained by the authorities is legitimate and relevant to a determination of the issue of whether there has been an interference. Indeed, bearing in mind the rapid pace of developments in the field of genetics and information technology, the Court cannot discount the possibility that in the future the private-life interests bound up with genetic information may be adversely affected in novel ways or in a manner which cannot be anticipated with precision today. Accordingly, the Court does not find any sufficient reason to depart from its finding in the *Van der Velden* case.** 72. **Legitimate concerns about the conceivable use of cellular material in the future are not, however, the only element to be taken into account in the determination of the present issue. In addition to the highly personal nature of cellular samples, the Court notes that they contain much sensitive information about an individual, including information about his or her health. Moreover, samples contain a unique genetic code of great relevance to both the individual and his relatives. In this respect the Court concurs with the opinion expressed by Baroness Hale in the House of Lords (see paragraph 25 above).**

73. **Given the nature and the amount of personal information contained in cellular samples, their retention *per se* must be regarded as interfering with the right to respect forthe private lives of the individuals concerned. That only a limited part of this information is actually extracted or used by the authorities through DNA profiling and that no immediate detriment is caused in a particular case does not change this conclusion (see *Amann*, cited above, § 69).**

75. The Court observes, nonetheless, that the profiles contain substantial amounts of unique personal data. While the information contained in the profiles may be considered objective and irrefutable in the sense submitted by the Government, their processing through automated means allows the authorities to go well beyond neutral identification. The Court notes in this regard that the Government accepted that DNA profiles could be, and indeed had in some cases been, used for familial searching with a view to identifying a possible genetic relationship between individuals. They also accepted the highly sensitive nature of such searching and the need for very strict controls in this respect. **In the Court's view, the DNA profiles' capacity to provide a means of identifying genetic relationships between individuals (see paragraph 39 above) is in itself sufficient to conclude that their retention interferes with the right to the private life of the individuals concerned. The frequency of familial searches, the safeguards attachedthereto and the likelihood of detriment in a particular case are immaterial in this respect (see *Amann*, cited above, § 69). This conclusion is similarly not affected by the fact that, since the information is in coded form, it is intelligible only with the use of computer technology and capable of being interpreted only by a limited number of persons.**

76. The Court further notes that it is not disputed by the Government that the processing of DNA profiles allows the authorities to assess the likely ethnic origin of the donor and that such techniques are in fact used in police investigations (see paragraph 40 above). **The** possibility the DNA profiles create for inferences to be drawn as to ethnic origin makes their retention all the more sensitive and susceptible of affecting the right to private life. This conclusion is consistent with the principle laid down in the Data Protection Convention and reflected in the Data Protection Act that both list personal data revealing ethnic origin among the special categories of sensitive data attracting a heightened level of protection (see paragraphs 30-31 and 41 above).

84. The Court is of the view that the general approach taken by the Convention organs in respect of photographs and voice samples should also be followed in respect of fingerprints. The Government distinguished the latter by arguing that they constituted neutral, objective and irrefutable material and, unlike photographs, were unintelligible tothe untutored eye and without a comparator fingerprint. While true, this consideration cannot alter the fact that fingerprints objectively contain unique information about theindividual concerned, allowing his or her identification with precision in a wide range of circumstances. They are thus capable of affecting his or her private life and the retention of this information without the consent of the individual concerned cannot be regarded as neutral or insignificant.

85. **The Court accordingly considers that the retention of fingerprints on the authorities' records in connection with an identified or**

		identifiable individual may in itself give rise, notwithstanding their objective and irrefutable character, to important private-life concerns. 105. The Court finds it to be beyond dispute that the fight against crime, and in particular against organised crime and terrorism, which is one of the challenges faced by today's European societies, depends to a great extent on the use of modern scientific techniques of investigation and identification. The techniques of DNA analysis were acknowledged by the Council of Europe more than fifteen years ago as offering advantages to the criminal-justice system (see Recommendation No. R (92) 1 of the Committee of Ministers, paragraphs 43-44 above). Nor is it disputed that the member States have since that time made rapid and marked progress in using DNA information in the determination of innocence or guilt. 112. The Court cannot, however, disregard the fact that, notwithstanding the advantages provided by comprehensive extension of the DNA database, other Contracting States have chosen to set limits on the retention and use of such data with a view to achieving a proper balance with the competing interests of preserving respect for private life. The Court observes that the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests. In the Court's view, the strong consensus existing among the Contracting States in this respect is of considerable importance and narrows the margin of appreciation left to the respondent State in the assessment of the permissible limits of the interference with private life in this sphere. The Court considers that any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard. 125. **In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society. This conclusion obviates the need for the Court to consider the applicants' criticism regarding the adequacy of certain particular safeguards, such as too broad an access to the personal data concerned and insufficient protection against the misuse or abuse of such data.**
43.	Eur. Court HR, *Bykov v. Russia*, judgment of 10 March 2009, 4378/02: secret services covert operations and surveillance; covert surveillance an interference with private life; lack of safeguards.	78. The Court has consistently held that when it comes to the interception of communications for the purpose of a police investigation, "the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence" (see *Malone v. the United Kingdom*, 2 August 1984, § 67, Series A no. 82). In particular, in order to comply with the requirement of the "quality of the law", a law which confers discretion must indicate the scope of that discretion, although the detailed procedures and conditions to be observed do not necessarily have to be incorporated in rules of substantive law. **The degree of precision required of the "law" in this**

		connection will depend upon the particular subject-matter. Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive – or to a judge – to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see, among other authorities, *Huvig v. France*, 24 April 1990, §§ 29 and 32, Series A no. 176-B;*Amann v. Switzerland* [GC], no. 27798/95, § 56, ECHR 2000-II; and *Valenzuela Contreras v. Spain*, 30 July 1998, § 46, *Reports of Judgments and Decisions* 1998-V). 80. **In the instant case, the applicant enjoyed very few, if any, safeguards in the procedure by which the interception of his conversation with V. was ordered and implemented. In particular, the legal discretion of the authorities to order the interception was not subject to any conditions, and the scope and the manner of its exercise were not defined; no other specific safeguards were provided for. Given the absence of specific regulations providing safeguards, the Court is not satisfied that, as claimed by the Government, the possibility for the applicant to bring court proceedings seeking to declare the "operative experiment" unlawful and to request the exclusion of its results as unlawfully obtained evidence met the above requirements.** 81. **It follows that in the absence of specific and detailed regulations, the use of this surveillance technique as part of an "operative experiment" was not accompanied by adequate safeguards against various possible abuses. Accordingly, its use was open to arbitrariness and was inconsistent with the requirement of lawfulness.**
44.	Eur. Court HR, *Szuluk v. The United Kingdom*, judgment of 2 June 2009, 36936/05: monitoring of prisoner's correspondence with doctor; no reason for monitoring; disproportionate intereference	**52. Furthermore, the Court does not consider the Prison Service's arguments as to the general difficulties involved in facilitating confidential medical correspondence for prisoners (see paragraph 14 above) to be of particular relevance to this case.** In the present case, the applicant only wished to correspond confidentially with one named medical specialist and the Court of Appeal accepted that her address and qualifications were easily verifiable. Moreover, the medical specialist in question appeared to have been willing and able to mark all correspondence with the applicant with a distinctive stamp, and had demonstrably done so prior to the prison governor's revision of his decision on 28 November 2002. The Court does not share the Court of Appeal's view that the risk that the applicant's medical specialist, whose bona fides was never challenged, might be "intimidated or tricked" into transmitting illicit messages was sufficient to justify the interference with the applicant's Article 8 rights in the exceptional circumstances of thepresent case. This is particularly so since the Court of Appeal further acknowledged that although the same risk was inherent in the case of secretarial staff of MPs (see paragraph 18 above), the importance of unimpeded correspondence with MPs outweighed that risk. 53. **In light of the severity of the applicant's medical condition, the Court considers that uninhibited correspondence with a medical specialist in the context of a prisoner suffering from a life-threatening condition should be afforded no less protection than the correspondence between a prisoner and an MP. In so finding, the Court refers to theCourt of Appeal's concession that it**

		might, in some cases, be disproportionate to refuse confidentiality to a prisoner's medical correspondence and the changes that have since been enacted to the relevant domestic law. The Court also has regard to the submissions of the applicant on this point, namely that the Government have failed to provide sufficient reasons why the risk of abuse involved in correspondence with named doctors whose exact address, qualifications and bona fides are not in question should be perceived as greater than the risk involved in correspondence with lawyers.
45.	Eur. Court HR, *Kvasnica v. Slovakia*, judgment of 9 June 2009, 72094/01: Ministry of interior taps lawyer's phone; telephone conversations and correspondence covered by Article 8; guidelins for surveillance not transparent	76. **Telephone conversations are covered by the notions of "private life" and "correspondence" within the meaning of Article 8. Their monitoring amounts to an interference with the exercise of one's rights under Article 8 (see, for example, *Lambert v. France*, 24 August 1998, § 21, *Reports of Judgments and Decisions* 1998-V).** 79. **In particular, the requirement of legal "foreseeability" in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. However, the domestic law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures. The Court has also stressed the need for safeguards in this connection. In its case-law on secret measures of surveillance, it has described an overview of the minimum safeguards that should be set out in statute law in order to avoid abuses of power (see *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, §§ 75-77, 28 June 2007 and *Weber and Saravia v. Germany* (dec.), no. 54934/00, ECHR 2006-..., with further references).** 86. **The respondent Government did not make available the relevant documents which were classified (see paragraph 75 above). On the basis of the documents before it the Court is not satisfied that the statutory conditions were complied with in their entirety in the applicant's case. For example, it has not been shown that the guarantees were met relating to the duration of the interference, whether there had been judicial control of the interception on a continuous basis, whether the reasons for the use of the devices remained valid, whether in practice measures were taken to prevent the interception of telephone calls between the applicant as a lawyer and criminal defendants as his clients. Similarly it has not been shown that the interference restricted the inviolability of applicant's home, the privacy of his correspondence and the privacy of information communicated only to an extent that was indispensable and that the information thus obtained was used exclusively for attaining the aim set out in section 36(1) of the Police Corps Act 1993.** **87. In addition, statements by several police officers and the judge involved are indicative of a number of shortcomings as regards the compliance with the relevant law in the applicant's case (see paragraphs 19, 20 and 25 above). In particular, the director of the special division of the financial and criminal police had concluded that the interference in issue had not been based on any specific suspicion against the applicant and no specific purpose had been indicated in the relevant request. In his written statement the Regional Court judge who had authorised the interception remarked**

		that similar requests were made in writing, but were submitted by the police investigators in person. The officer submitting the request presented the case orally and the oral presentation was usually more comprehensive than the written request. As requests for authorisation had to be handled with the utmost urgency, judges had no practical opportunity to examine the case file or to verify that the request for authorisation corresponded to the contents of the case file. Depositions of the four members of the financial police investigative team involved in the case included, *inter alia*, the information that the request for authorisation of the interception of the applicant's telephone had been drafted without a prior consultation of the case file. The documents before the Court contain no information indicating that those statements were unsubstantiated.
46.	Eur. Court HR, *Iordachi and others v. Moldova*, judgment of 14 September 2009, 25198/02: government surveillance of NGO communication; victimhood can be asserted without a measure necessarily being applied to a specific individual; domestic legislation lacked clarity and precision	29. **The Court reiterates that telephone communications are covered by the notions of "private life" and "correspondence" within the meaning of Article 8 (see *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 77, 29 June 2006, and the cases cited therein).** 34. T**he mere existence of the legislation entails, for all those who might fall within its reach, a menace of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunications services and thereby constitutes an "interference by a public authority" with the exercise of the applicants' right to respect for correspondence (see *Klass v. Germany*, cited above, § 41).** 39. The Court points out that recently, in its admissibility decision in *Weber and Saravia*, cited above, §§ 93-95, the Court summarised its case-law on the requirement of legal "foreseeability" in this field as follows: "93. **.... foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly (see, *inter alia*, *Leander v. Sweden,* judgment of 26 August 1987, Series A no. 116, p. 23, § 51). However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident (see, *inter alia Huvig*, cited above, pp. 54-55, § 29; and *Rotaru v. Romania* [GC], no. 28341/95, § 55, ECHR 2000-V). It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated (see *Kopp v. Switzerland*, judgment of 25 March 1998, *Reports* 1998-II, pp. 542-43, § 72, and *Valenzuela Contreras v. Spain*, judgment of 30 July 1998, *Reports* 1998-V, pp. 1924-25, § 46). The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (see *Kopp*, cited above, § 64;*Huvig*, cited above, § 29; and *Valenzuela Contreras*, ibid.).** 94. **Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against**

arbitrary interference (see, among other authorities, *Leander*, cited above, § 51; and *Huvig*, cited above, § 29).
95. In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed (see, *inter alia*, *Huvig*, cited above, § 34; *Valenzuela Contreras*, cited above, § 46; and *Prado Bugallo v. Spain*, no. 58496/00, § 30, 18 February 2003).”

40. Moreover, the Court recalls that in *Dumitru Popescu v. Romania* (cited above, paragraphs 70-73) the Court expressed the view that the body issuing authorisations for interception should be independent and that there must be either judicial control or control by an independent body over the issuing body's activity.

44. Still, the nature of the offences which may give rise to the issue of an interception warrant is not, in the Court's opinion, sufficiently clearly defined in the impugned legislation. In particular, the Court notes that more than one half of the offences provided for in the Criminal Code fall within the category of offences eligible for interception warrants (see paragraph 14 above). Moreover, the Court is concerned by the fact that the impugned legislation does not appear to define sufficiently clearly the categories of persons liable to have their telephones tapped. It notes that Article 156 § 1 of the Criminal Code uses very general language when referring to such persons and states that the measure of interception may be used in respect of a suspect, defendant or other person involved in a criminal offence. No explanation has been given as to who exactly falls within the category of “other person involved in a criminal offence”.

45. The Court further notes that the legislation in question does not provide for a clear limitation in time of a measure authorising interception of telephone communications. While the Criminal Code imposes a limitation of six months (see paragraph 17 above), there are no provisions under the impugned legislation which would prevent the prosecution authorities from seeking and obtaining a new interception warrant after the expiry of the statutory six months' period.

46. Moreover, it is unclear under the impugned legislation who – and under what circumstances – risks having the measure applied to him or her in the interests of, for instance, protection of health or morals or in the interests of others. While enumerating in section 6 and in Article 156 § 1 the circumstances in which tapping is susceptible of being applied, the Law on Operational Investigative Activities and the Code of Criminal Procedure fails, nevertheless, to define “national security”, “public order”, “protection of health”, “protection of morals”, “protection of the rights and interests of others”, “interests of ... the economic situation of the country” or “maintenance of legal order” for the purposes of interception of telephone communications. Nor does the legislation specify the circumstances in which an individual may be at risk of having his telephone communications intercepted on any of those grounds.

47. As to the second stage of the procedure of interception of telephone communications, it would appear that the investigating judge plays a very limited role. According to Article 41 of the Code of Criminal Procedure, his

role is to issue interception warrants. According to Article 136 of the same Code, the investigating judge is also entitled to store "the original copies of the tapes along with the complete written transcript ... in a special place in a sealed envelope" and to adopt "a decision regarding the destruction of records which are not important for the criminal case". However, the law makes no provision for acquainting the investigating judge with the results of the surveillance and does not require him or her to review whether the requirements of the law have been complied with. On the contrary, section 19 of the Law on Operational Investigative Activities appears to place such supervision duties on the "Prosecutor General, his or her deputy, and the municipal and county prosecutors". Moreover, in respect of the actual carrying out of surveillance measures in the second stage, it would appear that the interception procedure and guarantees contained in the Code of Criminal Procedure and in the Law on Operational Investigative Activities are applicable only in the context of pending criminal proceedings and do not cover the circumstances enumerated above.

48. Another point which deserves to be mentioned in this connection is the apparent lack of regulations specifying with an appropriate degree of precision the manner of screening the intelligence obtained through surveillance, or the procedures for preserving its integrity and confidentiality and the procedures for its destruction (see, as examples*a contrario*, *Weber and Saravia*, cited above, §§ 45-50).

49. The Court further notes that overall control of the system of secret surveillance is entrusted to the Parliament which exercises it through a specialised commission (see section 18 of the Law on Operational Investigative Activities). However, the manner in which the Parliament effects its control is not set out in the law and the Court has not been presented with any evidence indicating that there is a procedure in place which governs the Parliament's activity in this connection.

50. **As regards the interception of communications of persons suspected of offences, the Court observes that in *Kopp* (cited above, § 74) it found a violation of Article 8 because the person empowered under Swiss secret surveillance law to draw a distinction between matters connected with a lawyer's work and other matters was an official of the Post Office's legal department. In the present case, while the Moldovan legislation, like the Swiss legislation, guarantees the secrecy of lawyer-client communications (see paragraph 18 above), it does not provide for any procedure which would give substance to the above provision. The Court is struck by the absence of clear rules defining what should happen when, for example, a phone call made by a client to his lawyer is intercepted.**

51. **The Court notes further that in 2007 the Moldovan courts authorised virtually all the requests for interception made by the prosecuting authorities (see paragraph 13 above). Since this is an uncommonly high number of authorisations, the Court considers it necessary to stress that telephone tapping is a very serious interference with a person's rights and that only very serious reasons based on a reasonable suspicion that the person is involved in serious criminal activity should be taken as a basis for authorising it.** The Court notes that the Moldovan legislation does not elaborate on the degree of reasonableness of the suspicion against a person for the purpose of authorising an interception. Nor does it contain safeguards other than the one provided for in section 6(1), namely that interception should take place only when it is otherwise impossible to achieve the aims. This, in the Court's opinion, is a matter of concern when looked at against the very

		high percentage of authorisations issued by investigating judges. For the Court, this could reasonably be taken to indicate that the investigating judges do not address themselves to the existence of compelling justification for authorising measures of secret surveillance.
47.	Eur. Court HR *Haralambie v. Romania* judgment of 27 October 2009, 21737/03: access to secret service documentation; retention of information on applicants political and economic position; positive obligation on state to ensure access in a reasonable time	**Judgment in French** From the Legal Summary: Article 8: In the context of access to personal files held by the public authorities, the authorities had a duty to provide individuals with an "effective and accessible procedure" for obtaining access to "all relevant and appropriate information". Domestic law gave every Romanian citizen the right to access their personal file held by the *Securitate* and other documents or information on them. The Romanian Intelligence Service and other institutions in possession of those files were obliged to guarantee the right of access to the files and to send them to the CNSAS at the latter's request. Domestic law had thus formally established an administrative procedure for gaining access to files. With regard to the effectiveness of that procedure, it should be noted that it was not until 2008 that the applicant had been invited to consult his personal file, which was more than six years after his initial request made in 2002 and five years after the CNSAS had informed him that a file on him existed. Furthermore, it was not until the application had been communicated to the Government that the applicant obtained a reply to his request. It was clear from the materials in the case file that the file on the applicant had been sent to the CNSAS in 2005. Whilst the law had not initially provided for a time-limit for transferring the file, the legislative change enacted in 2006 established a time-limit of sixty days for transferring files. The length of the administrative procedure in question had far exceeded the time-limit required under the 2006 Act. Moreover, having regard to the applicant's advanced age, the Court found that his interest in retracing his personal history during the era of the totalitarian regime was all the more urgent. Further, the Court did not accept that the quantity of files transferred or the shortcomings in the archive system could of themselves justify a delay of more than six years by the institutions concerned in granting the applicant's request. Having regard to the foregoing, the State had not satisfied the positive obligation incumbent on it to provide the applicant with an effective and accessible procedure allowing him to obtain access to his personal file within a reasonable time. Discussion of violation of Article 8 in §§ 74-97 76. Dans ses observations complémentaires soumises le 22 octobre 2008, après que le requérant ait eu accès à son fichier personnel, le Gouvernement conteste l'applicabilité de l'article 8, alléguant que les données contenues dans ce fichier ne concernaient pas sa vie privée, mais sa collaboration avec l'ancienne *Securitate* et la manière dont il avait accompli les obligations en découlant. 77. La Cour rappelle que les données de nature publique peuvent relever de la vie privée lorsqu'elles sont d'une manière systématique, recueillies et mémorisées dans des fichiers tenus par les pouvoir publics. Cela vaut davantage encore lorsque ces données concernent le passé lointain d'une personne (*Rotaru* précité, § 34 et *Rad*, précité, § 34). En outre, la Cour a jugé que le respect de la vie privée englobe le droit pour l'individu de nouer et développer des relations avec ses semblables et qu'aucune raison de principe ne permet d'exclure les activités professionnelles de la notion de « vie privée » (*Rotaru* précité § 43 et *mutatis mutandis Sidabras et Džiautas c. Lituanie*, nos 55480/00 et59330/00, §§ 48-49, CEDH 2004-VIII).

Enfin, la Cour a déjà souligné la concordance entre cette interprétation extensive et celle de la Convention élaborée au sein du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, du 28 janvier 1981, entrée en vigueur pour la Roumanie le 1er juin 2002, dont le but est « de garantir (...) à toute personne physique (...) le respect (...) notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant » (article 1), ces dernières étant définies dans l'article 2 comme « toute information concernant une personne physique identifiée ou identifiable » (arrêt *Amann c. Suisse* [GC], no 27798/95, § 65, CEDH 2000-II et *Rotaru* précité 43).

78. En l'espèce, le requérant fut informé par le CNSAS, le 28 mars 2003, qu'il avait fait l'objet de mesures de surveillance par la *Securitate* et qu'il y avait un fichier à son nom.
Plus précisément, la note classée à la page 20 dudit fichier attachée « aux fins d'exploitation » à un courrier datant du 23 novembre 1989 (voir paragraphe 24, ci-dessus), indiquait que le requérant, lors de conversations avec son entourage, avait fait des commentaires défavorables à l'égard de la situation économique et politique du pays et qu'il avait colporté le contenu hostile des émissions du poste de radio l'*Europe libre* (*Europa liberă*), tout en exprimant ses convictions relatives au pluralisme des partis politiques.

79. Or, il est évident que, tant le fait de conserver, après les avoir recueillis, de tels renseignements dans un fichier tenu par des agents de l'État, que l'intérêt du requérant d'avoir accès au contenu de ce fichier relèvent de la « vie privée » au sens de l'article 8 § 1 de la Convention (voir *Rotaru* précité § 44 et *Rad,* précité, § 34). En l'occurrence, il s'agissait pour l'intéressé de se voir communiquer des informations le concernant et dont il ignorait de toute évidence la nature exacte aussi longtemps qu'il n'y avait pas accès. Dès lors, il convenait qu'il puisse prendre connaissance de ces données, le cas échéant de caractère personnel, voire intime, et dont le caractère éventuellement inexact pouvait risquer de porter atteinte à sa réputation (voir *mutatis mutandis Gunes c. France*, no 32157/06, § 26, 20 novembre 2008). Cela d'autant plus qu'il ressort du préambule de la loi no 187/1999 que le but de ces fichiers était de terroriser la population de sorte qu'il était légitime, dans ces conditions, que le requérant ait pensé que les informations collectées pouvaient toucher aux aspects les plus intimes de sa vie privée.
Dans ces conditions, la Cour estime que l'article 8 trouve à s'appliquer en l'espèce.
2. Sur l'observation de l'article 8

80. Le requérant reproche à l'État de ne pas lui avoir donné accès à son fichier personnel créé par la *Securitate*, avant 1989, en dépit du fait que, tant la loi interne que l'institution principalement chargée de l'appliquer, à savoir le CNSAS, lui reconnaissaient un tel droit.

81. Dans ses premières observations présentées le 4 juillet 2008, le Gouvernement a indiqué qu'il n'y a pas eu refus d'accès au fichier, mais seulement un obstacle objectif découlant de l'impossibilité d'identifier le dossier et, ensuite, des doutes existant quant à l'identité de la personne faisant l'objet du fichier.

82. Le Gouvernement a indiqué également que « le contrôle des informations n'avait pas pu être réalisé directement pas le CNSAS qui ne se trouvait pas en possession de tous les dossiers ». En ce qui concerne l'obligation prévue par l'article 20 de la loi no 187/1999, de remettre au CNSAS tous les dossiers de l'ancienne *Securitate*, le Gouvernement a fait

valoir que le délai prévu par la loi a été prorogé par l'article IV du règlement d'urgence du Gouvernement no 16/2006, délai qui a été, en principe, respecté.

83. Dans ses observations supplémentaires du 22 octobre 2008, après que le requérant ait eu accès audit fichier, le Gouvernement a fait valoir que le retard constaté en l'espèce avait été causé par des raisons objectives, notamment des défaillances du système d'archivage et le nombre élevé de fichiers personnels gardés par le Service roumain de renseignements et non par la mauvaise foi des autorités. Le Gouvernement souligne également que le CNSAS a effectué toutes les démarches prévues par la loi afin de parvenir à l'identification du fichier concernant le requérant et estime que le retard en question n'est pas constitutif d'une atteinte à sa vie privée.

84. La Cour rappelle qu'aux exigences plutôt négatives contenues dans l'article 8 de la Convention, qui tend pour l'essentiel à prémunir l'individu contre des ingérences arbitraires des pouvoirs publics, peuvent s'ajouter des obligations positives inhérentes à un respect effectif de la vie privée (*Roche c. Royaume-Uni* [GC], no 32555/96, § 157, CEDH 2005-X). La frontière entre les obligations positives et négatives de l'État au titre de l'article 8 ne se prête pas à une définition précise, mais les principes applicables sont comparables (*Odièvre c. France* [GC], no 42326/98, § 40, CEDH 2003-III).

85. S'agissant de l'accès à des fichiers personnels détenus par les pouvoirs publics, en dehors du contexte des renseignements sensibles pour la sécurité nationale comme dans l'affaire *Leander c. Suède*, (26 mars 1987, § 51, série A no 116), la Cour a reconnu un intérêt primordial, protégé par la Convention, aux personnes désireuses d'obtenir les renseignements qu'il leur faut pour connaître et comprendre leur enfance et leurs années de formation (*Gaskin c. Royaume-Uni*, 7 juillet 1989, § 49, série A no 160) ou pour retracer leur identité personnelle, s'agissant en particulier de leur filiation naturelle (*Odièvre* précité, §§ 41-47) ou des renseignements sur les risques pour la santé auxquels les intéressés avaient été exposés (*Roche*, précité, § 161 et *Guerra et autres c. Italie*, 19 février 1998, § 60, *Recueil des arrêts et décisions* 1998-I).

86. La Cour a considéré, dans ce contexte, que pesait sur les autorités une obligation positive d'offrir aux intéressés une « procédure effective et accessible » qui leur permette d'avoir accès à « l'ensemble des informations pertinentes et appropriées » (*Roche*, précité, § 162, *McGinley et Egan c. Royaume-Uni*, 9 juin 1998, § 101, *Recueil des arrêts et décisions* 1998-III).

87. Dans la présente affaire, le requérant se plaint de ne pas lui avoir donné accès aux renseignements figurant dans le fichier tenu par le SRI et que ces renseignements auraient été abusivement gardés par ce dernier, en dépit de l'obligation découlant de la loi no 187/1999 de les mettre à la disposition du CNSAS afin d'assurer aux personnes intéressées l'exercice effectif de leur droit d'accès. En s'élevant contre ce refus, le requérant se plaint en substance non d'un acte, mais de l'inaction de l'État (*Gaskin* précité, § 41).

88. La Cour note que le droit interne, à savoir l'article 1er de la loi no 187/1999, puis l'article 1er du règlement d'urgence no 24/2008 qui l'a remplacée, consacrait le droit de tout citoyen roumain d'accéder au fichier personnel tenu par la *Securitate* et à d'autres documents et informations visant sa personne (voir paragraphe 31, ci-dessus). En outre, l'article 20 de la loi no 187/1999, tout comme l'article 31 du règlement d'urgence

no 24/2008, prévoient que le SRI et les autres institutions possédant les archives en question étaient obligées de garantir ce droit d'accès auxdits fichiers et de les remettre au CNSAS sur demande de ce dernier.

89. Par ces dispositions, la loi interne a formellement instauré une procédure administrative d'accès aux fichiers (voir aussi la décision *Rad*, précité, §§ 35 et 42). Reste à déterminer si, dans le cas du requérant, cette procédure a été effective.

90. En l'espèce, dès le 28 mars 2003, le CNSAS informa le requérant qu'il avait fait l'objet de mesures de surveillance par la *Securitate* et qu'il y avait un fichier identifié à son nom, mais qu'il y avait certaines difficultés pour le retrouver.

91. La Cour note cependant que ce n'est que le 21 mai 2008 que le requérant a été invité à consulter son fichier personnel, soit plus de six ans après sa première demande datant du 18 mars 2002 et cinq ans après que le CNSAS l'ait informé du fait qu'un fichier à son nom avait été identifié. En outre, la Cour constate que ce n'est qu'après la communication de la requête au Gouvernement que le requérant a obtenu une réponse à sa demande (*Bourdov c. Russie*, no 59498/00, § 36, CEDH 2002-III). Or, il ressort des pièces du dossier (voir paragraphe 20, ci-dessus) que le fichier identifié au nom du requérant avait été remis au CNSAS le 19 octobre 2005.

92. Dans la mesure où le Gouvernement indique comme principale cause de ce retard le manquement du SRI, au détriment du requérant, à son obligation de transférer les archives en question vers le CNSAS, la Cour note que, dans un premier temps, la loi ne prévoyait aucun délai pour l'accomplissement du transfert. Ce ne fut que par le changement législatif intervenu en 2006, auquel le Gouvernement fait référence, qu'un délai de soixante jours fut fixé pour le transfert des archives.

93. La Cour constate ainsi que la durée de la procédure administrative en cause a largement dépassé le délai imposé par la loi de 2006. Or, si le législateur a fixé un délai de trente jours pour que le CNSAS réponde aux intéressés et, lors de la modification de la loi intervenue en 2006, un délai de soixante jours pour que le SRI et d'autres institutions concernées remettent les archives en question, c'est de toute évidence qu'à ses yeux, une telle procédure devait être menée avec une célérité particulière (voir *mutatis mutandis Nichifor c. Roumanie (no 1)*, no 62276/00, § 28, 13 juillet 2006 et *Gunes c. France*, no 32157/06, § 26, 20 novembre 2008).
En outre, compte tenu de l'âge avancé du requérant, la Cour estime que son intérêt de retracer son parcours personnel lors de l'époque du régime totalitaire était d'autant plus urgent.

94. Dans la mesure où le Gouvernement indique qu'au moins pendant une certaine période, le fichier en cause était introuvable, la Cour note qu'il ressort des éléments du dossier (voir paragraphe 23, ci-dessus) que ledit fichier a été microfilmé le 23 juillet 1996, donc il était déjà disponible autrement qu'en format papier et que, de toute manière, le fichier était en possession du CNSAS dès le 19 octobre 2005.

95. En outre, la Cour ne saurait considérer que la quantité de fichiers transférés – qui était de seulement 3 573 fichiers en 2002-2003, pour passer à 249 803 fichiers transmis par le SRI en 2006 et 15 500 fichiers en 2008 (voir les paragraphes 46-48, ci-dessus) – ou les défaillances du système d'archivage, y compris l'erreur matérielle concernant la date de naissance du requérant commise dans le fichier personnel identifié à son nom, pourraient à eux seuls justifier un retard de plus de six ans de la part

		des institutions concernées, pour faire droit à la demande du requérant. 96. Compte tenu de ce qui précède, la Cour estime que l'État n'a pas satisfait à l'obligation positive qui lui incombait d'offrir au requérant une procédure effective et accessible pour lui permettre d'avoir accès dans un délai raisonnable à son fichier personnel (voir *mutatis mutandis, Roche*, précité, §§ 166-167 et *mutatis mutandis Kenedi c. Hongrie*, no31475/05, § 48, 26 mai 2009). Partant, il y a eu violation de l'article 8 de la Convention. 97. S'agissant du prétendu manquement des autorités à présenter au requérant l'ensemble des documents de son fichier personnel, notamment ceux qui auraient concerné la période de 1970 à 1975 à laquelle deux notes qu'il a pu consulter font référence (voir le paragraphe 26, ci-dessus), compte tenu des informations qui lui ont été soumises par les parties, la Cour n'est pas en mesure de prendre position sur l'éventuelle existence d'autres documents concernant le requérant. Compte tenu de ce fait et du constat auquel la Cour est arrivée au paragraphe 96, ci-dessus, quant à l'inefficacité de la procédure d'accès au fichier personnel, elle estime qu'il n'y a pas lieu à examiner séparément le prétendu manquement des autorités à présenter au requérant l'ensemble des documents de son fichier personnel (voir *mutatis mutandis, Roche,* précité, § 168).
48.	Eur. Court HR, *B.B. v. France, Gardel v. France, M.B. v. France*, judgments of 17 December 2009, 5335/06, 16428/05, 22115/06: sexual offendors' database; lengthy retention of data not disproportionate to aim pursued – prevention of recidivism and assistance with investigations	58. As to the rest, the Court observes that the Sex Offenders Register contains data concerning the applicant's private life. The register comes under the responsibility of the Ministry of Justice and is supervised by the judge who manages the criminal records. The Court stresses that it is not its task at this stage to speculate on the sensitive nature or otherwise of the information gathered or on the possible difficulties experienced by the applicant. **According to its case-law, the storing by a public authority of information relating to an individual's private life amounts to interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding (see, *mutatis mutandis*, *Leander*, cited above, § 48, and *Kopp v. Switzerland*, 25 March 1998, § 53, *Reports* 1998-II). More specifically, the Court has already ruled that the requirement for persons convicted of sexual offences to inform the police of their name, date of birth, address or change of address falls within the scope of Article 8 § 1 of the Convention (see*Adamson*, cited above).** 62. The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention. **The domestic law must therefore afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article (see, *mutatis mutandis*, *Z v. Finland*, 25 February 1997, § 95, *Reports* 1997-I). In line with its findings in *S. and Marper v. the United Kingdom* ([GC], nos. 30562/04 and30566/04, § 103, ECHR 2008), the Court is of the view that the need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored and that they are preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored (see paragraphs 27 and 28 above, in particular Article 5 of the Data Protection Convention and the Preamble thereto and Principle 7 of Recommendation No. R (87) 15 of the Committee of Ministers**

		regulating the use of personal data in the police sector). The domestic law must also afford adequate guarantees to ensure that retained personal data are efficiently protected from misuse and abuse. 63. **The Court cannot call into question the preventive purpose of a register such as the one on which the applicant was placed after being sentenced to fifteen years' imprisonment for the rape of a minor. The aim of that register, as it has already pointed out, is to prevent crime and in particular to combat recidivism and, in such cases, to make it easier to identify offenders.** Sexual abuse is unquestionably an abhorrent type of wrongdoing, with debilitating effects on its victims. Children and other vulnerable individuals are entitled to State protection, in the form of effective deterrence, from such grave types of interference with essential aspects of their private lives (see *Stubbings and Others v. the United Kingdom*, 22 October 1996, § 64, *Reports* 1996-IV). 66. As to the obligation to provide proof of address every six months and of any change of address, on pain of a prison sentence and payment of a fine, the Court has previously held that this did not give rise to an issue from the standpoint of Article 8 of the Convention (see *Adamson*, cited above). 69. The Court considers that this judicial procedure for the removal of data provides for independent review of the justification for retention of the information according to defined criteria (see *S. and Marper*, cited above, § 119) and affords adequate and effective safeguards of the right to respect for private life, having regard to the seriousness of the offences giving rise to placement on the register. Admittedly, the storing of the data for such a long period could give rise to an issue under Article 8 of the Convention. However, the Court notes that the applicant will in any event have a practical opportunity of lodging an application for removal of the stored data from the date on which the decision giving rise to their entry in the register ceases to have effect. In these circumstances, the Court is of the view that the period of time for which the data are kept is not disproportionate to the aim pursued in storing the information. 70. As to the rules on the use of the register and the range of public authorities which have access to it, the Court notes that the latter has been extended on several occasions and is no longer limited to the judicial authorities and the police; administrative bodies now also have access (Article 706-53-7 of the CCP, see paragraph 18 above). The fact remains, nevertheless, that the register may only be consulted by authorities that are bound by a duty of confidentiality, and in precisely defined circumstances. In addition, the present case does not lend itself to examination *in concreto* of the issue of the availability of the register for consultation for administrative purposes.
49.	Eur. Court HR, *Uzun v. Germany*, judgment of 2 September 2010, 35623/05: GPS surveillance by law enforcement; GPS surveillance interferes with Article 8; GPS movements in public places less intrusive than telecoms surveillance; adequate	44. **There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor (see *Perry*, cited above, § 37).** A person walking along the street will inevitably be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character (see also *Herbecq and the Association "Ligue des droits de*

	and effective safeguards in place	*l'homme" v. Belgium*, nos. 32200/96 and 32201/96, Commission decision of 14 January 1998, Decisions and Reports (DR) 92-B, p. 92, concerning the use of photographic equipment which does not involve the recording of the visual data obtained). Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain (see *P.G. and J.H. v. the United Kingdom*, cited above, § 57; *Peck*, cited above, §§ 58-59; and *Perry*, cited above, § 38). 46. **Thus, the Court has considered that the systematic collection and storing of data by security services on particular individuals, even without the use of covert surveillance methods, constituted an interference with these persons' private lives** (see *Rotaru v. Romania* [GC], no. 28341/95, §§ 43-44, ECHR 2000-V; *P.G. and J.H. v. the United Kingdom*, cited above, § 57; *Peck*, cited above, § 59; and *Perry*, cited above, § 38; compare also *Amann v. Switzerland* [GC], no. 27798/95, §§ 65-67, ECHR 2000-II, where the storing of information about the applicant on a card in a file was found to be an interference with private life, even though it contained no sensitive information and had probably never been consulted). The Court has also referred in this context to the Council of Europe's Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data, which came into force – *inter alia* for Germany – on 1 October 1985 and whose purpose is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such data being defined as "any information relating to an identified or identifiable individual" (Article 2) (see *P.G. and J.H. v. the United Kingdom*, cited above, § 57). 47. The Court has further taken into consideration whether the impugned measure amounted to a processing or use of personal data of a nature to constitute an interference with respect for private life (see, in particular, *Perry*, cited above, §§ 40-41). Thus, it considered, for instance, the permanent recording of footage deliberately taken of the applicant at a police station by a security camera and its use in a video identification procedure as the processing of personal data about the applicant interfering with his right to respect for private life (ibid., §§ 39-43). Likewise, the covert and permanent recording of the applicants' voices at a police station for further analysis as voice samples directly relevant for identifying these persons in the context of other personal data was regarded as the processing of personal data about them amounting to an interference with their private lives (see *P.G. and J.H. v. the United Kingdom*, cited above, §§ 59-60; and *Perry*, cited above, § 38). 48. Finally, the publication of material obtained in public places in a manner or degree beyond that normally foreseeable may also bring recorded data or material within the scope of Article 8 § 1 (see *Peck*, cited above, §§ 60-63, concerning disclosure to the media for broadcast use of video footage of the applicant taken in a public place; and *Perry*, cited above, § 38). 52. **In the Court's view, GPS surveillance is by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings. Having regard to the principles established in its case-law, it nevertheless finds the above-mentioned factors sufficient to conclude that the applicant's observation via GPS, in the circumstances, and the**

processing and use of the data obtained thereby in the manner described above amounted to an interference with his private life as protected by Article 8 § 1

61. As to the requirement of legal "foreseeability" in this field, the Court reiterates that in the context of covert measures of surveillance, the law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to any such measures (see, among other authorities, *Malone v. the United Kingdom*, 2 August 1984, § 67, Series A no. 82; *Valenzuela Contreras v. Spain*, 30 July 1998, § 46 (iii), *Reports* 1998-V; and *Bykov v. Russia*[GC], no. 4378/02, § 76, ECHR 2009-...). In view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is particularly precise, especially as the technology available for use is continually becoming more sophisticated (see *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 93, ECHR 2006-XI; *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, § 75, 28 June 2007; *Liberty and Others v. the United Kingdom*, no.58243/00, § 62, 1 July 2008; and *Iordachi and Others v. Moldova*, no. 25198/02, § 39, 10 February 2009).

63. In addition, in the context of secret measures of surveillance by public authorities, because of the lack of public scrutiny and the risk of misuse of power, compatibility with the rule of law requires that domestic law provides adequate protection against arbitrary interference with Article 8 rights (see, *mutatis mutandis*, *Amann*, cited above, §§ 76-77;*Bykov*, cited above, § 76; see also *Weber and Saravia* (dec.), cited above, § 94; and *Liberty and Others*, cited above, § 62). The Court must be satisfied that there exist adequate and effective guarantees against abuse. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law (see*Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 77, with reference to *Klass and Others v. Germany*, 6 September 1978, § 50, Series A no. 28).

65. As to the law's foreseeability and its compliance with the rule of law, the Court notes at the outset that in his submissions, the applicant strongly relied on the minimum safeguards which are to be set out in statute law in order to avoid abuses as developed by the Court in the context of applications concerning the interception of telecommunications. According to these principles, the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their communications monitored; a limit on the duration of such monitoring; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which data obtained may or must be erased or the records destroyed, have to be defined in statute law (see *Weber and Saravia*, cited above, § 95, with further references).

66. While the Court is not barred from gaining inspiration from these principles, it finds that these rather strict standards, set up and applied in the specific context of surveillance of telecommunications (see also *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 76; *Liberty and Others*, cited above, § 62; and *Iordachi and Others*, cited above, § 39), are not applicable as such to

cases such as the present one, concerning surveillance via GPS of movements in public places and thus a measure which must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations (see paragraph 52 above). It will therefore apply the more general principles on adequate protection against arbitrary interference with Article 8 rights as summarised above (see paragraph 63).

69. In examining whether domestic law contained adequate and effective guarantees against abuse, the Court observes that in its nature conducting surveillance of a person by building a GPS receiver into the car he or she uses, coupled with visual surveillance of that person, permits the authorities to track that person's movements in public places whenever he or she is travelling in that car. It is true that, as the applicant had objected, there was no fixed statutory limit on the duration of such monitoring. A fixed time-limit had only subsequently been enacted in so far as under the new Article 163f § 4 of the Code of Criminal Procedure, the systematic surveillance of a suspect ordered by a Public Prosecutor could not exceed one month, and any further extension could only be ordered by a judge (see paragraph 32 above). However, the Court is satisfied that the duration of such a surveillance measure was subject to its proportionality in the circumstances and that the domestic courts reviewed the respect of the proportionality principle in this respect (see for an example paragraph 28 above). It finds that German law therefore provided sufficient guarantees against abuse on that account.

72. The Court considers that such judicial review and the possibility to exclude evidence obtained from an illegal GPS surveillance constituted an important safeguard, as it discouraged the investigating authorities from collecting evidence by unlawful means. In view of the fact that GPS surveillance must be considered to interfere less with a person's private life than, for instance, telephone tapping (an order for which has to be made by an independent body both under domestic law (see Article 100b § 1 of the Code of Criminal Procedure, paragraph 30 above) and under Article 8 of the Convention (see, in particular, *Dumitru Popescu v. Romania (no. 2)*, no. 71525/01, §§ 70-71, 26 April 2007, and *Iordachi and Others*, cited above, § 40), the Court finds subsequent judicial review of a person's surveillance by GPS to offer sufficient protection against arbitrariness. Moreover, Article 101 § 1 of the Code of Criminal Procedure contained a further safeguard against abuse in that it ordered that the person concerned be informed of the surveillance measure he or she had been subjected to under certain circumstances (see paragraph 31 above).

73. The Court finally does not overlook that under the Code of Criminal Procedure, it was not necessary for a court to authorise and supervise surveillance via GPS which was carried out in addition to other means of surveillance and thus all surveillance measures in their entirety. It takes the view that sufficient safeguards against abuse require, in particular, that uncoordinated investigation measures taken by different authorities must be prevented and that, therefore, the prosecution, prior to ordering a suspect's surveillance via GPS, had to make sure that it was aware of further surveillance measures already in place. However, having also regard to the findings of the Federal Constitutional Court on this issue (see paragraph 27 above), it finds that at the relevant time the safeguards in place to prevent a person's total surveillance, including the principle of proportionality, were sufficient to prevent abuse.

78. In determining whether the applicant's surveillance via GPS as carried out in the present case was “necessary in a democratic society”, the Court reiterates that the notion of necessity implies that the interference

		corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued (see *Leander v. Sweden*, 26 March 1987, § 58, Series A no. 116; and *Messina v. Italy (no. 2)*, no. 25498/94, § 65, ECHR 2000-X). In examining whether, in the light of the case as a whole, the measure taken was proportionate to the legitimate aims pursued, the Court notes that the applicant's surveillance via GPS was not ordered from the outset. The investigation authorities had first attempted to determine whether the applicant was involved in the bomb attacks at issue by measures which interfered less with his right to respect for his private life. They had notably tried to determine the applicant's whereabouts by installing transmitters in S.'s car, the use of which (other than with the GPS) necessitated the knowledge of where approximately the person to be located could be found. However, the applicant and his accomplice had detected and destroyed the transmitters and had also successfully evaded their visual surveillance by State agents on many occasions. Therefore, it is clear that other methods of investigation, which were less intrusive than the applicant's surveillance by GPS, had proved to be less effective. 80. The Court considers that in these circumstances, the applicant's surveillance via GPS had led to a quite extensive observation of his conduct by two different State authorities. In particular, the fact that the applicant had been subjected to the same surveillance measures by different authorities had led to a more serious interference with his private life, in that the number of persons to whom information on his conduct had become known had been increased. Against this background, the interference by the applicant's additional surveillance via GPS thus necessitated more compelling reasons if it was to be justified. However, the GPS surveillance was carried out for a relatively short period of time (some three months), and, as with his visual surveillance by State agents, affected him essentially only at weekends and when he was travelling in S.'s car. Therefore, he cannot be said to have been subjected to total and comprehensive surveillance. Moreover, the investigation for which the surveillance was put in place concerned very serious crimes, namely several attempted murders of politicians and civil servants by bomb attacks. As shown above, the investigation into these offences and notably the prevention of further similar acts by the use of less intrusive methods of surveillance had previously not proved successful. Therefore, the Court considers that the applicant's surveillance via GPS, as carried out in the circumstances of the present case, was proportionate to the legitimate aims pursued and thus "necessary in a democratic society" within the meaning of Article 8 § 2.
50.	Eur. Court HR, *Kennedy v. The United Kingdom*, judgment of 18 May 2010, 26839/05: law enforcement surveillance of business communications; applicant does not need to concretely demonstrate surveillance mea	**118. It is not disputed that mail, telephone and email communications, including those made in the context of business dealings, are covered by the notions of "private life" and "correspondence" in Article 8 § 1.** 120. The Court's approach to assessing whether there has been an interference in cases raising a general complaint about secret surveillance measures was set out in its *Klass and Others* judgment, cited above, §§ 34 to 38 and 41: "34. ... The question arises in the present proceedings whether an individual is to be deprived of the opportunity of lodging an application with the Commission because, owing to the secrecy of the measures objected to, he cannot point to any concrete measure specifically affecting him. In the Court's view, the effectiveness (l'effet utile) of the Convention implies in such circumstances some possibility of having access

to the Commission. If this were not so, the efficiency of the Convention's enforcement machinery would be materially weakened. The procedural provisions of the Convention must, in view of the fact that the Convention and its institutions were set up to protect the individual, be applied in a manner which serves to make the system of individual applications efficacious.
The Court therefore accepts that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him. The relevant conditions are to be determined in each case according to the Convention right or rights alleged to have been infringed, the secret character of the measures objected to, and the connection between the applicant and those measures.
35. In the light of these considerations, it has now to be ascertained whether, by reason of the particular legislation being challenged, the applicants can claim to be victims ... of a violation of Article 8 ... ofthe Convention ...
36. The Court points out that where a State institutes secret surveillance the existence of which remains unknown to the persons being controlled, with the effect that the surveillance remains unchallengeable, Article 8 ... could to a large extent be reduced to a nullity. It is possible in such a situation for an individual to be treated in a manner contrary to Article 8 ..., or even to be deprived of the right granted by that Article ..., without his being aware of it and therefore without being able to obtain a remedy either at the national level or before the Convention institutions.
...
The Court finds it unacceptable that the assurance of the enjoyment of a right guaranteed by the Convention could be thus removed by the simple fact that the person concerned is kept unaware of its violation. A right of recourse to the Commission for persons potentially affected by secret surveillance is to be derived from Article 25 ..., since otherwise Article 8 ... runs the risk of being nullified.

152. The Court has held on several occasions that the reference to "foreseeability" in the context of interception of communications cannot be the same as in many other fields (see *Malone*, cited above, § 67; *Leander v. Sweden*, 26 March 1987, § 51, Series A no. 116; *Association for European Integration*, cited above, § 79; and *Al-Nashif*, cited above, § 121). In its admissibility decision in *Weber and Saravia*, cited above, §§ 93 to 95, the Court summarised its case-law on the requirement of legal "foreseeability" in this field:
"93. ... foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly (see, *inter alia*, *Leander* [*v. Sweden,* judgment of 26 August 1987, Series A no. 116], p. 23, § 51). However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident (see, *inter alia*, *Malone*, cited above, p. 32, § 67; *Huvig*, cited above, pp. 54-55, § 29; and *Rotaru*). It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated (see *Kopp v. Switzerland*, judgment of 25 March 1998, *Reports* 1998-II, pp. 542-43, § 72, and *Valenzuela Contreras v. Spain*, judgment of 30 July 1998, *Reports* 1998-V, pp. 1924-25, § 46). The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which

and the conditions on which public authorities are empowered to resort to any such measures (see *Malone*, ibid.; *Kopp*, cited above, p. 541, § 64; *Huvig*, cited above, pp. 54-55, § 29; and *Valenzuela Contreras*, ibid.).

94. Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to therule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on thecompetent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see, among other authorities, *Malone*, cited above, pp. 32-33, § 68; *Leander*, cited above, p. 23, § 51; and *Huvig*, cited above, pp. 54-55, § 29).

95. In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of theoffences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed (see, *inter alia*, *Huvig*, cited above, p. 56, § 34; *Amann*, cited above, § 76; *Valenzuela Contreras*, cited above, pp. 1924-25, § 46; and *Prado Bugallo v. Spain*, no. 58496/00, § 30, 18 February 2003)."

153. As to the question whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, the Court recalls that powers to instruct secret surveillance of citizens are only tolerated under Article 8 to the extent that they are strictly necessary for safeguarding democratic institutions. In practice, this means that there must be adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of thepossible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by thenational law (see *Klass and Others*, cited above, §§ 49 to 50; and *Weber and Saravia*, cited above, § 106).

156. In order to assess whether the RIPA provisions meet the foreseeability requirement, the Court must first examine whether the provisions of the Code can be taken into account insofar as they supplement and further explain the relevant legislative provisions. In this regard, the Court refers to its finding in Silver and Others v. the United Kingdom, 25 March 1983, §§ 88 to 89, Series A no. 61 that administrative orders and instructions concerning the scheme for screening prisoners' letters established a practice which had to be followed save in exceptional circumstances and that, as a consequence, although they did not themselves have the force of law, to the extent to which those concerned were made sufficiently aware of their contents they could be taken into account in assessing whether the criterion of foreseeability was satisfied in the application of the Prison Rules.

159. As to the nature of the offences, the Court emphasises that the condition of foreseeability does not require States to set out

exhaustively by name the specific offences which may give rise to interception. However, sufficient detail should be provided of the nature of the offences in question. In the case of RIPA, section 5 provides that interception can only take place where the Secretary of State believes that it is necessary in the interests of national security, for the purposes of preventing or detecting serious crime or for the purposes of safeguarding the economic well-being of the United Kingdom (see paragraphs 31 to 32 above). The applicant criticises the terms "national security" and "serious crime" as being insufficiently clear. **The Court disagrees. It observes that the term "national security" is frequently employed in both national and international legislation and constitutes one of the legitimate aims to which Article 8 § 2 itself refers. The Court has previously emphasised that the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all conduct that may prompt a decision to deport an individual on "national security" grounds. By the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance (*Al-Nashif*, cited above, § 121). Similar considerations apply to the use of the term in the context of secret surveillance.** Further, additional clarification of how the term is to be applied in practice in the United Kingdom has been provided by the Commissioner, who has indicated that it allows surveillance of activities which threaten the safety or well-being of the State and activities which are intended to undermine or overthrow Parliamentary democracy by political, industrial or violent means (see paragraph 33 above). As for "serious crime", this is defined in the interpretative provisions of the Act itself and what is meant by "detecting" serious crime is also explained in the Act (see paragraphs 34 to 35 above). **TheCourt is of the view that the reference to serious crime, together with the interpretative clarifications in the Act, gives citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to secret surveillance measures.** The Court therefore considers that, having regard to theprovisions of RIPA, the nature of the offences which may give rise to an interception order is sufficiently clear (compare and contrast *Iordachi and Others*, cited above, § 46).

161. In respect of the duration of any telephone tapping, the Act clearly stipulates, first, the period after which an interception warrant will expire and, second, the conditions under which a warrant can be renewed (see paragraph 50 to 51 above). Although a warrant can be renewed indefinitely, the Secretary of State himself must authorise any renewal and, upon such authorisation, must again satisfy himself that the warrant remains necessary on the grounds stipulated in section 5(3) (see paragraph 51 above). In thecontext of national security and serious crime, the Court observes that the scale of the criminal activities involved is such that their planning often takes some time. Subsequent investigations may also be of some duration, in light of the general complexity of such cases and the numbers of individuals involved. **The Court is therefore of the view that theoverall duration of any interception measures will depend on the complexity and duration of the investigation in question and, provided that adequate safeguards exist, it is not unreasonable to leave this matter for the discretion of the relevant domestic authorities.** The Code explains that the person seeking the renewal must make an application tothe Secretary of State providing an update and assessing the value of the interception operation to date. He must specifically address why he considers that the warrant remains necessary on section 5(3) grounds (see paragraph 54 above). Further, under section 9(3) RIPA, the Secretary

of State is obliged to cancel a warrant where he is satisfied that the warrant is no longer necessary on section 5(3) grounds (see paragraph 52 above). There is also provision in the Act for specific factors in the schedule to thewarrant to be deleted where the Secretary of State considers that they are no longer relevant for identifying communications from or to the interception subject (see paragraph 53 above). The Code advises that the duty on the Secretary of State to cancel warrants which are no longer necessary means, in practice, that intercepting agencies must keeptheir warrants under continuous review (see paragraph 55 above). The Court concludes that the provisions on duration, renewal and cancellation are sufficiently clear.

162. As regards the procedure for examining, using and storing the data, the Government indicated in their submissions that, under RIPA, an intercepting agency could, in principle, listen to all intercept material collected (see paragraph 144 above). **The Court recalls its conclusion in *Liberty and Others*, cited above, § 65, that the authorities' discretion to capture and listen to captured material was very wide.** However, that case, unlike the present case, involved external communications, in respect of which data were captured indiscriminately. Contrary to the practice under the Interception of Communications Act 1985 concerning external communications, interception warrants for internal communications under RIPA relate to one person or one set of premises only (cf. *Liberty and Others*, cited above, § 64), thereby limiting the scope of the authorities' discretion to intercept and listen to private communications. Moreover, any captured data which are not necessary for any of the authorised purposes must be destroyed.

167. The Court recalls that it has previously indicated that in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge (see *Klass and Others*, cited above, § 56). In the present case, the Court highlights the extensive jurisdiction of the IPT to examine any complaint of unlawful interception. Unlike in many other domestic systems (see, for example, the G 10 Law discussed in the context of *Klass and Others* and *Weber and Saravia*, both cited above), any person who suspects that his communications have been or are being intercepted may apply to the IPT (see paragraph 76 above). The jurisdiction of the IPT does not, therefore, depend on notification to the interception subject that there has been an interception of his communications. The Court emphasises that the IPT is an independent and impartial body, which has adopted its own rules of procedure. The members ofthe tribunal must hold or have held high judicial office or be experienced lawyers (see paragraph 75 above). In undertaking its examination of complaints by individuals, the IPT has access to closed material and has the power to require the Commissioner to provide it with any assistance it thinks fit and the power to order disclosure by those involved inthe authorisation and execution of a warrant of all documents it considers relevant (see paragraph 78 above). In the event that the IPT finds in the applicant's favour, it can, *inter alia*, quash any interception order, require destruction of intercept material and order compensation to be paid (see paragraph 80 above). The publication of the IPT's legal rulings further enhances the level of scrutiny afforded to secret surveillance activities in the United Kingdom (see paragraph 89 above).

168. Finally, the Court observes that the reports of the Commissioner scrutinise any errors which have occurred in the operation of the legislation. In his 2007 report, theCommissioner commented that none of the breaches or errors identified were deliberate and that, where

		interception had, as a consequence of human or technical error, unlawfully taken place, any intercept material was destroyed as soon as the error was discovered (see paragraph 73 above). There is therefore no evidence that any deliberate abuse of interception powers is taking place. 169. **In the circumstances, the Court considers that the domestic law on interception of internal communications together with the clarifications brought by the publication ofthe Code indicate with sufficient clarity the procedures for the authorisation and processing of interception warrants as well as the processing, communicating and destruction of intercept material collected.** The Court further observes that there is no evidence of any significant shortcomings in the application and operation of the surveillance regime. Onthe contrary, the various reports of the Commissioner have highlighted the diligence with which the authorities implement RIPA and correct any technical or human errors which accidentally occur (see paragraphs 62, 67, 71 and 73 above). Having regard to the safeguards against abuse in the procedures as well as the more general safeguards offered by the supervision of the Commissioner and the review of the IPT, the impugned surveillance measures, insofar as they may have been applied to the applicant in thecircumstances outlined in the present case, are justified under Article 8 § 2.
51.	Eur. Court HR *Mikolajová v. Slovakia*, judgment of 18 January 2011, 4479/03: police report; unclear storage terms; illegal disclosure of the report to a third party; reputation	57. Given the **gravity of the conclusion contained in the police decision**, namely that the applicant was guilty of a violent criminal offence, coupled with the **uncontested disclosure of the impugned decision to a third party** (health insurance company), the Court finds that there **has been an "interference" with her rights under Article 8 of the Convention.** ... the Court lays emphasis on the fact that the applicant was **never charged with or proved to have committed any criminal offence.** It follows that the text of the police decision **cannot be considered to be the foreseeable consequence of the applicant's own doing**, precisely because she has never been charged with, let alone proved, to have committed any crime. 61. ... **For the Court, the damage which may be caused to the reputation of the individual concerned through the communication of inaccurate or misleading information cannot be ignored either.** The Court would also observe with concern that the **authorities have not indicated whether the police decision remains valid indefinitely, such as to constitute, with each communication to a third party, assuming such to be in pursuit of a legitimate aim, a continuing threat to the applicant's right to reputation.** 62. In examining whether the domestic authorities have complied with the above-mentioned fair balance requirement, the Court must have regard to the safeguards in place in order to avoid arbitrariness in decision-making and to secure the rights of the individual against abuse. **In the instant case, the Court cannot but note the lack of any available recourse through which the applicant could obtain a subsequent retraction or clarification of the terms of the police decision.** The Court further notes that in the above‑mentioned Babjak case the original police decision which stated that that applicant had committed a crime had been superseded by a subsequent official statement from the competent police department unequivocally clarifying that it had not been proved that he had committed any criminal offence. 63. Having regard to the above considerations, the Court finds that the domestic authorities failed to strike a fair balance between the applicant's

		Article 8 rights and any interests relied on by the Government to justify the terms of the police decision and its disclosure to a third party. There has accordingly been a breach of Article 8 of the Convention.
52.	Eur. Court HR *Dimitrov-Kazakov v. Bulgaria,* judgment of 10 February 2011, 11379/03: police register; non-convicted individual; storage of data in police files	33. En l'espèce, la Cour note que l'ingérence litigieuse était fondée sur l'instruction no 1-90 du 24 décembre 1993 sur l'enregistrement de police des personnes ayant commis des infractions pénales. Il n'est pas contesté que cette instruction, non publique à l'époque des faits, revêtait un caractère confidentiel et qu'elle était réservée, jusqu'à son déclassement en 2004, à l'usage interne du ministère des Affaires intérieures, de sorte que le requérant n'a pas pu en prendre connaissance pour en prévoir les conséquences. **La Cour relève que l'activité d'enregistrement de police a été visée dans une loi accessible au public seulement à partir du mois de décembre 1997, soit après l'ouverture du dossier relatif au requérant (paragraphe 20 ci-dessus). Dès lors, la « loi » interne ne répondait pas à l'exigence d'accessibilité prévue à l'article 8 § 2 de la Convention.** L'enregistrement de police en cause n'était donc pas prévu par la loi au sens de l'article 8. Partant, il y a eu violation de cette disposition. 34. Eu égard à la conclusion qui précède, la Cour n'estime pas nécessaire de vérifier en l'espèce le respect des autres exigences de l'article 8 § 2.
53.	Eur. Court HR, *Shimovolos v. Russia*, judgment of 21 June 2011, 30194/09: surveillance database, quality of the law	69. Turning to the present case, the Court observes that the creation and maintenance of the Surveillance Database and the procedure for its operation are governed by ministerial order no. 47 (see paragraph 42 above). **That order is not published and is not accessible to the public. The grounds for registration of a person's name in the database, the authorities competent to order such registration, the duration of the measure, the precise nature of the data collected, the procedures for storing and using the collected data and the existing controls and guarantees against abuse are thus not open to public scrutiny and knowledge.** 70. For the above reasons, the Court does not consider that the domestic law indicates with sufficient clarity the scope and manner of exercise of the discretion conferred on the domestic authorities to collect and store in the Surveillance Database information on persons' private lives. In particular, **it does not, as required by the Court's case-law, set out in a form accessible to the public any indication of the minimum safeguards against abuse.** The interference with the applicant's rights under Article 8 was not, therefore, "in accordance with the law".
54.	Eur. Court HR *Khelili v. Switzerland*, judgment of 18 October 2011, application no. 16188/07: registration in police register as a "prostitute," request for recitification/erasure, lack of clear proof that situation remedied	68. La Cour ne sous-estime aucunement l'importance d'une prévention efficace de la criminalité. Toutefois, compte tenu de ce qui précède, et notamment eu égard à l'importance primordiale de la présomption d'innocence dans une société démocratique (voir, dans ce sens, S. et Marper c. Royaume-Uni précité, § 122), **elle ne saurait accepter que le maintien de la mention « prostituée » comme profession de la requérante, qui n'a jamais été condamnée pour exercice illicite de la prostitution au sens de l'article 199 du code pénal (paragraphe 23 ci-dessus), puisse passer pour répondre à un « besoin social impérieux » au sens de l'article 8 de la Convention.** Ni les autorités internes ni le Gouvernement n'ont par ailleurs allégué que la suppression de la mention litigieuse du dossier de police était impossible ou difficile pour des raisons techniques. 69. En outre, il convient de rappeler que le 15 juillet 2005, le chef de la police du canton de Genève a confirmé que la mention « prostituée » devait être corrigée (paragraphe 13 ci-dessus). Toutefois, le 24 juin 2006,

		la requérante a appris, lors d'une conversation téléphonique avec un service non indiqué de la même police qu'elle figurait toujours comme « prostituée » (paragraphe 15 ci-dessus). Il ressort également de l'arrêt du tribunal de police de l'arrondissement de La Broye et du Nord vaudois du 15 mars 2007 que, par une lettre du coordinateur suisse du Centre de coopération policière et douanière du 26 juillet 2005, la requérante aurait obtenu la radiation dans les fichiers de cet organisme de certains faits la concernant, « sans toutefois que l'on sache précisément de quels faits il s'agissait » (paragraphe 19 ci-dessus). **70. Au vu de ces incertitudes, du comportement contradictoire des autorités, du principe selon lequel il appartient à ces mêmes autorités d'apporter la preuve de l'exactitude d'une donnée (article 3A § 2 LDP, paragraphe 22 ci-dessus), de la marge d'appréciation réduite dont jouissaient les autorités internes en la matière et de la gravité de l'ingérence dans le droit de la requérante, la Cour estime que le maintien de la mention « prostituée » dans le dossier de police pendant des années n'était pas nécessaire dans une société démocratique**
55.	Eur. Court HR, *Gillberg v. Sweden*, judgment of 03 April 2012, 41723/06: criminal convictions and reputation, foreseeability	67. The applicant maintained that the criminal conviction in itself affected the enjoyment of his "private life" by prejudicing his honour and reputation. **The Court reiterates in this regard that Article 8 cannot be relied on in order to complain of a loss of reputation which is the foreseeable consequence of one's own actions such as, for example, the commission of a criminal offence** (see, inter alia, Sidabras and Džiautas v. Lithuania, nos. 55480/00 and 59330/00, § 49, ECHR 2004-VIII, and Mikolajová v. Slovakia, no. 4479/03, § 57, 18 January 2011). No violation of Art. 8 found.
56.	Eur. Court HR, *Nada v. Switzerland*, judgment of 12 September 2012, 10593/08: UN Sanctions implemented in national law, terrorist database, lack of criminal convictions, entry ban, not enough effort to have the applicant de-listed	149. The applicant complained that the measure by which he was prohibited from entering or passing through Switzerland had breached his right to respect for his private life, including his professional life, and his family life. **He contended that this ban had prevented him from seeing his doctors in Italy or in Switzerland and from visiting his friends and family. He further claimed that the addition of his name to the list annexed to the Taliban Ordinance had impugned his honour and reputation.** Issue of the measures being "necessary in a democratic society" 180. **In view of the foregoing, the Court finds that Switzerland enjoyed some latitude, which was admittedly limited but nevertheless real, in implementing the relevant binding resolutions of the United Nations Security Council.** 193. It should be pointed out in this connection that, under paragraph 2(b) of Resolution 1390 (2002), **the Sanctions Committee was entitled to grant exemptions in specific cases,** especially for medical, humanitarian or religious reasons. During the meeting of 22 February 2008 (see paragraph 54 above), a representative of the Federal Department of Foreign Affairs indicated that the applicant could request the Sanctions Committee to grant a broader exemption in view of his particular situation. The applicant did not make any such request, but **it does not appear, in particular from the record of that meeting, that the Swiss authorities offered him any assistance to that end.** 194. It has been established that the applicant's name was added to the United Nations list, not on the initiative of Switzerland but on that of the United States of America. Neither has it been disputed that, at least until the adoption of Resolution 1730 (2006), it was for the State of citizenship or residence of the person concerned to approach the Sanctions

		Committee for the purposes of the delisting procedure. Indeed, in the applicant's case Switzerland was neither his State of citizenship nor his State of residence, **and the Swiss authorities were not therefore competent to undertake such action. However, it does not appear that Switzerland ever sought to encourage Italy to undertake such action or to offer it assistance for that purpose** (see, mutatis mutandis, the case of Sayadi and Vinck (Human Rights Committee), § 12, paragraphs 88 to 92 above). It can be seen from the record of the meeting of 22 February 2008 (see paragraph 54 above) that the authorities merely suggested that the applicant contact the Italian Permanent Mission to the United Nations, adding that Italy at that time had a seat on the Security Council. 195. The Court acknowledges that Switzerland, along with other States, made considerable efforts that resulted, after a few years, in improvement to the sanctions regime (see paragraphs 64 and 78 above). It is of the opinion, however, in view of the principle that the Convention protects rights that are not theoretical or illusory but practical and effective (see Artico, cited above, § 33), that it is important in the present case to consider the measures that the national authorities actually took, or sought to take, in response to the applicant's very specific situation. **In this connection, the Court considers in particular that the Swiss authorities did not sufficiently take into account the realities of the case, especially the unique geographical situation of Campione d'Italia, the considerable duration of the measures imposed or the applicant's nationality, age and health.** It further finds that the possibility of deciding how the relevant Security Council resolutions were to be implemented in the domestic legal order **should have allowed some alleviation of the sanctions regime applicable to the applicant,** having regard to those realities, in order to avoid interference with his private and family life, without however circumventing the binding nature of the relevant resolutions or compliance with the sanctions provided for therein. 196. In the light of the Convention's special character as a treaty for the collective enforcement of human rights and fundamental freedoms (see, for example, Soering, cited above, § 87, and Ireland v. the United Kingdom, 18 January 1978, § 239, Series A no. 25**), the Court finds that the respondent State could not validly confine itself to relying on the binding nature of Security Council resolutions, but should have persuaded the Court that it had taken – or at least had attempted to take – all possible measures to adapt the sanctions regime to the applicant's individual situation.**
57.	Eur. Court of HR., *M.M. v. the United Kingdom*, judgment of 13 November 2012, 24029/07: data on caution, unclear storage and disclosure terms, lack of independent review of disclosure of information	205. As regards specifically the fact that the retention policy changed after the administration of the applicant's caution, the Court notes that the applicant consented to the administration of the caution on the basis that it would be deleted from her record after five years. … However, the Court expresses concern about the change in policy, which occurred several years after the applicant had accepted the caution and which was to have significant effects on her employment prospects. **206. In the present case, the Court highlights the absence of a clear legislative framework for the collection and storage of data, and the lack of clarity as to the scope, extent and restrictions of the common law powers of the police to retain and disclose caution data. It further refers to the absence of any mechanism for independent review of a decision to retain or disclose data,** either under common law police powers or pursuant to Part V of the 1997 Act. Finally, the Court notes the limited filtering arrangements in respect of disclosures made

		under the provisions of the 1997 Act: as regards mandatory disclosure under section 113A, no distinction is made on the basis of the nature of the offence, the disposal in the case, the time which has elapsed since the offence took place or the relevance of the data to the employment sought. **207. The cumulative effect of these shortcomings is that the Court is not satisfied that there were, and are, sufficient safeguards in the system for retention and disclosure of criminal record data to ensure that data relating to the applicant's private life have not been, and will not be, disclosed in violation of her right to respect for her private life.** The retention and disclosure of the applicant's caution data accordingly cannot be regarded as being in accordance with the law.
58.	Eur. Court of HR., *M.K. v. France* judgment of 18 April 2013, 19522/09: fingerprint retention over long period of time of individuals never convicted, unclear definition of offences which can lead to finerprint collection and storage, right to deletion illusory	20. The applicant complained that his right to respect for his private life had been infringed by the retention of personal data on him in the national fingerprint database. 40. It also notes that the public prosecutor's refusal to delete the prints taken during the second set of proceeding was motivated by the need to protect the applicant's interests by ruling out his involvement should someone else attempt to steal his identity (see paragraph 12 above). **Besides the fact that such a reason is not explicitly mentioned in the provisions of Article 1 of the impugned decree, barring a particularly extensive interpretation of this Article, the Court considers that accepting the argument based on an alleged guarantee of protection against potential identity theft would in practice be tantamount to justifying the storage of information on the whole population of France, which would most definitely be excessive and irrelevant.** 41. Moreover, in addition to the primary function of the database, which is to facilitate efforts to find and identify the perpetrators of serious crimes and other major offences, the decree mentions another function, namely to facilitate "the prosecution, investigation and trial of cases referred to the judicial authority", **without specifying whether this is confined to serious crimes and other major offences.** It also covers "persons who have been charged in criminal proceedings and whose identification is required" (Article 3-2 of the decree), and so can embrace all offences de facto, including mere summary offences, in the hypothesis that this would help identify the perpetrators of crimes and offences as specified in Article 1 of the Decree (see paragraph 17 above). At all events, the circumstances of the case, which concerned book theft and was discontinued, show that the instrument applies to minor offences. The instant case is thus very different from those specifically relating to such serious offences as organised crime (see S. and Marper, cited above) or sexual assault (see Gardel, B.B. v. France and M.B. v. France, cited above). 42. **Furthermore, the Court notes that the decree draws no distinction based on whether or not the person concerned has been convicted by a court, or has even been prosecuted.** In S. and Marper, the Court highlighted the risk of stigmatisation, stemming from the fact that persons who had either been acquitted or had their cases discontinued - and were therefore entitled to the presumption of innocence – were treated in the same way as convicted persons (ibid., § 22). The situation in the instant case is similar on this point, as the applicant was acquitted and discharged in an initial set of proceedings, and subsequently had the charges against him dropped. 43. In the Court's view, the provisions of the impugned decree on the procedure for the retention of data also fail to provide sufficient protection for the persons in question.

		44. In connection with the possibility of deleting such data, the Court considers that the right at any time to submit a deletion request to the court is liable, in the words of the 25 August 2006 order, to conflict with the interests of the investigating authorities, which require access to a database with as many references as possible (see paragraph 14 above). **Accordingly, since the interests at stake are contradictory, if only partially, the deletion, which is not in fact a right, provides a safeguard which is "theoretical and illusory" rather than "practical and effective".** 45. The Court notes that while the retention of information stored in the file is limited in time, it nevertheless extends to twenty-five years. Having regard to its previous finding that the chances of deletion requests succeeding are at best hypothetical, **a twenty-five-year time-limit is in practice tantamount to indefinite retention, or at least, as the applicant contends, a standard period rather than a maximum one.** 46. In conclusion, the Court considers that the respondent State has overstepped its margin of appreciation in this matter, as the regulations on the retention in the impugned database of the fingerprints of persons suspected of having committed offences but not convicted, as applied to the applicant in the instant case, do not strike a fair balance between the competing public and private interests at stake. **Consequently, the retention of the data must be seen as a disproportionate interference with the applicant's right to respect for his private life and cannot be regarded as necessary in a democratic society.**
59.	Eur. Court of HR., *Avilkina and Others v. Russia* judgment of 6 June 2013 1585/09: prosecutor collection of information. Further disclosure of sensitive/medical information	51. Referring to the unlimited power of the prosecutor to request the disclosure of confidential medical information, the courts found the disclosure to be in compliance with the law and dismissed the applicants' claims. **The Court discerns no mention in the text of the judgments of any efforts by the national authorities' to strike a fair balance between the applicants' right to respect for their private life and the prosecutor's activities aimed at protecting public health and individuals' rights in that field.** Nor did the authorities adduce relevant or sufficient reasons which would have justified the disclosure of the confidential information. **52. Accordingly, in the Court's view the opportunity to object to the disclosure of the confidential medical information once it was already in the prosecutor's possession did not afford the applicants sufficient protection against unauthorised disclosure.** 53. The above considerations are sufficient for the Court to conclude that the collection by the prosecutor's office of confidential medical information concerning the applicants **was not accompanied by sufficient safeguards to prevent disclosure inconsistent with the respect for the applicants' private life guaranteed under Article 8 of the Convention.**
60.	Eur. Court of HR., *Brunet v. France* judgment of 18 September 2014, 21010/10: registration of data in police database, lack of effective remedies, data deletion	24. Le requérant allègue que son inscription au STIC constitue une violation de la Convention 42. **De même, elle note qu'à l'époque des faits la décision du procureur de la République n'était susceptible d'aucun recours.** Certes, d'une part, le droit interne permet désormais à l'intéressé d'adresser une nouvelle demande au magistrat référent visé à l'article 230-9 du code de procédure pénale, comme le soutient le Gouvernement. La Cour observe néanmoins que le texte précise que ce magistrat « dispose

		des mêmes pouvoirs d'effacement, de rectification ou de maintien des données personnelles (...) que le procureur de la République». **Aux yeux de la Cour, un tel recours ne présente donc pas le caractère d'effectivité nécessaire, l'autorité décisionnaire ne disposant d'aucune marge d'appréciation quant à la pertinence du maintien des informations au fichier, notamment lorsque la procédure a été classée sans suite après une médiation pénale, comme en l'espèce.** D'autre part, la jurisprudence récente du Conseil d'État reconnaît la possibilité d'exercer un recours pour excès de pouvoir contre les décisions du procureur en matière d'effacement ou de rectification, qui ont pour objet la tenue à jour du STIC et sont détachables d'une procédure judiciaire (paragraphe 19 ci-dessus). **Cependant, la Cour constate que cette faculté n'était pas reconnue à l'époque des faits, le requérant s'étant vu expressément notifier l'absence de toute voie de contestation ouverte contre la décision du procureur du 1er décembre 2009.** 43. Ainsi, bien que la conservation des informations insérées dans le STIC soit limitée dans le temps, il en découle que **le requérant n'a pas disposé d'une possibilité réelle de demander l'effacement des données le concernant et que, dans une hypothèse telle que celle de l'espèce, la durée de vingt ans prévue est en pratique assimilable, sinon à une conservation indéfinie, du moins à une norme plutôt qu'à un maximum (M.K., précité).** 44. En conclusion, la Cour estime que l'État défendeur a outrepassé sa marge d'appréciation en la matière, le régime de conservation des fiches dans le STIC, tel qu'il a été appliqué au requérant, ne traduisant pas un juste équilibre entre les intérêts publics et privés concurrents en jeu. Dès lors, la conservation litigieuse s'analyse en une atteinte disproportionnée au droit du requérant au respect de sa vie privée et ne peut passer pour nécessaire dans une société démocratique.
61.	Eur. Court of HR., *Dragojević v. Croatia*, judgment of 15 January 2015, 68955/11: secret telephone surveillance, judicial scrutiny, remedies, safeguards, unclear scope of discreation	67. The applicant complained that the secret surveillance of his telephone conversations had been in violation of the guarantees of Article 8 of the Convention **98. Moreover, the Court considers that in a situation where the legislature envisaged prior detailed judicial scrutiny of the proportionality of the use of secret surveillance measures, a circumvention of this requirement by retrospective justification, introduced by the courts, can hardly provide adequate and sufficient safeguards against potential abuse since it opens the door to arbitrariness by allowing the implementation of secret surveillance contrary to the procedure envisaged by the relevant law.** 99. This is particularly true in cases where **the only effective possibility for an individual** subjected to covert surveillance in the context of criminal proceedings **is to challenge the lawfulness of the use of such measures before the criminal courts** during the criminal proceedings against him or her (see paragraph 72 above). ... 100. ... **At the same time, the Government have not provided any information on remedies** – such as an application for a declaratory judgment or an action for damages – **which may become available to a person in the applicant's situation** (see Association for European Integration and Human Rights and Ekimdzhiev, cited above, § 102). 101. Against the above background, the Court finds that the relevant domestic law, as **interpreted and applied by the competent courts, did**

		not provide reasonable clarity regarding the scope and manner of exercise of the discretion conferred on the public authorities, and in particular did not secure in practice adequate safeguards against various possible abuses. Accordingly, the procedure for ordering and supervising the implementation of the interception of the applicant's telephone was **not shown to have fully complied with the requirements of lawfulness, nor was it adequate to keep the interference with the applicant's right to respect for his private life and correspondence to what was "necessary in a democratic society".**
62.	Eur. Court of HR., *R.E. v. the United Kingdom,* 27 October 2015, 62498/11: surveillance of legal consultations between a lawyer and a client at a police station, RIPA assessment, foreseeability	122. In the special context of secret surveillance measures, the Court has found that "foreseeability" requires that domestic law be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (see, for example, the admissibility decision in Weber and Saravia v. Germany (dec.), no. 54934/00, § 93, ECHR 2006-XI). This is very similar to – and at times considered together with – the test for deciding whether an interference is "necessary in a democratic society" in pursuit of a legitimate aim; namely, whether the minimum safeguards set out in statute law in order to avoid abuses of power are adequate (see Klass and Others v. Germany, cited above, § 50; and Weber and Saravia v. Germany, cited above, § 95). 127. It is true that the Court has generally only applied the strict criteria in Valenzuela-Contreras in the context of interception of communication cases. However, **it has suggested that the precision required by the legislation will depend on all the circumstances of the case and, in particular, the level of interference with the individual's rights under Article 8 of the Convention.** **130. The Court has not, therefore, excluded the application of the principles developed in the context of interception cases in covert-surveillance cases; rather, it has suggested that the decisive factor will be the level of interference with an individual's right to respect for his or her private life and not the technical definition of that interference.** **131. The present case concerns the surveillance of legal consultations taking place in a police station, which the Court considers to be analogous to the interception of a telephone call between a lawyer and client. The Court has recognised that, while Article 8 protects the confidentiality of all correspondence between individuals, it will afford "strengthened protection" to exchanges between lawyers and their clients, as lawyers would be unable to defend their clients if they were unable to guarantee that their exchanges would remain confidential** (Michaud v. France, no. 12323/11, § 118, ECHR 2012). The Court therefore considers that the surveillance of a legal consultation constitutes an extremely high degree of intrusion into a person's right to respect for his or her private life and correspondence; higher than the degree of intrusion in Uzun and even in Bykov. Consequently, in such cases it will expect the same safeguards to be in place to protect individuals from arbitrary interference with their Article 8 rights as it has required in cases concerning the interception of communications, at least insofar as those principles can be applied to the form of surveillance in question. 132. The Court has emphasised that although sufficient detail should be provided of the nature of the offences in question, the condition of foreseeability does not require States to set out exhaustively by name the specific offences which may give rise to interception (see, for example,

Kennedy v. the United Kingdom, cited above, § 159). In Part II of RIPA, section 32 provides that intrusive surveillance can take place where the Secretary of State or senior authorising officer believes it is necessary in the interests of national security, for the purposes of preventing or detecting serious crime, or in the interests of the economic well-being of the United Kingdom. In this respect it is almost identical to section 5 in Part I of RIPA. Paragraph 4.12 of the Revised Code further clarifies that where the surveillance is likely to result in the acquisition of knowledge of matters subject to legal privilege, it is subject to an enhanced authorisation regime and the circumstances in section 32 will arise only in a very restricted range of cases, such as where there is a threat to life or limb, or to national security, and the surveillance is reasonably regarded as likely to yield intelligence necessary to counter that threat see paragraph 75 above).

133. In Kennedy, the Court accepted that the reference to national security and serious crime in section 5, together with the interpretative clarifications in RIPA, gave citizens an adequate indication as to the circumstances in which and the conditions on which public authorities were empowered to resort to interception. As noted in Kennedy, though the term "national security" is not defined in RIPA, it is frequently employed in national and international legislation and constitutes one of the legitimate aims to which Article 8 § 2 itself refers. The terms "serious crime" and "detecting" are defined in the interpretive provisions of RIPA (see paragraphs 57 and 58 above), which apply to both Part I and Part II. In fact, the only discernible difference between the authorisation of the interception of communications provided for in Part I and the authorisation of intrusive surveillance in Part II is that under Part I authorisation is given by the Secretary of State whereas under Part II it may be given by a senior authorising officer (see paragraph 49 above). However, in view of the fact that authorisation by a senior authorising officer generally only takes effect when it has been approved by the Surveillance Commissioner, an independent officer who must have held high judicial office (see paragraph 76 above), the Court does not consider that this fact by itself merits a departure from its conclusions in Kennedy. Consequently, the Court considers that, having regard to the provisions of RIPA, the nature of the offences which may give rise to intrusive surveillance is sufficiently clear.

134. RIPA does not provide any limitation on the persons who may be subjected to intrusive surveillance. Indeed, it is clear from section 27(3) that the conduct that may be authorised under Part II includes conduct outside the United Kingdom. However, as indicated in paragraphs 48 – 49 above, the RIPA regime does set out the relevant circumstances which can give rise to intrusive surveillance, which in turn provides guidance as to the categories of person likely in practice to be subject to such surveillance (see also Kennedy, cited above, § 160). As already noted, those circumstances are further restricted where the surveillance is intended to result in the acquisition of knowledge of matters subject to legal privilege (see paragraph 75 above).

136. Bearing in mind the fact that intrusive surveillance under Part II of RIPA concerns the covert surveillance of anything taking place on residential premises or in private vehicles by a person or listening device, the Court accepts that it will not necessarily be possible to know in advance either on what premises the surveillance will take place or what individuals will be affected by it. However, Part II requires the application to set out in full the information that is known, and the proportionality of the measure will subsequently be scrutinised at two separate levels (by the senior authorising officer and by the Surveillance Commissioner). In

the circumstances, the Court considers that no further clarification of the categories of persons liable to be subject to secret surveillance can reasonably be required.

137. With regard to the duration of intrusive surveillance, unless renewed a written authorisation will cease to have effect after three months from the time it took effect (see paragraph 66 above). The senior authorising officer or designated deputy may grant a renewal for a period of three months if it is considered necessary for the authorisation to continue for the purpose for which it was issued; however, except in urgent cases the authorisation will only take effect once it has been approved by a Surveillance Commissioner (see paragraph 67 above). Applications for renewal must record whether it is the first renewal or every occasion on which the authorisation was previously renewed; any significant changes to the information contained in the original application; the reason why it is necessary to continue with intrusive surveillance; the content and value to the investigation or operation of the product so far obtained by the authorisation; and the results of any reviews of the investigation or operation. Furthermore, regular reviews of all authorisations must be undertaken and the senior authorising officer who granted or last renewed an authorisation must cancel it if he or she is satisfied that it no longer meets the criteria upon which it was authorised (see paragraph 68 above). The Court therefore considers that the provisions of Part II of RIPA and the Revised Code which deal with duration, renewal and cancellation are sufficiently clear.

138. In contrast, fewer details concerning the procedures to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating the data to other parties, and the circumstances in which recordings may or must be erased or the tapes destroyed are provided in Part II of RIPA and/or the Revised Code. Although material obtained by directed or intrusive surveillance can normally be used in criminal proceedings and law enforcement investigations, paragraph 4.23 of the Revised Code makes it clear that material subject to legal privilege which has been deliberately acquired cannot be so used (see paragraph 75 above). Certain other safeguards are included in Chapter 4 of the Revised Code with regard to the retention and dissemination of material subject to legal privilege (see paragraph 75 above). Paragraph 4.25 of the Revised Code provides that where legally privileged material has been acquired and retained, the matter should be reported to the authorising officer by means of a review and to the relevant Commissioner or Inspector during his next inspection. The material should be made available during the inspection if requested. Furthermore, where there is any doubt as to the handling and dissemination of knowledge of matters which may be subject to legal privilege, Paragraph 4.26 of the Revised Code states that advice should be sought from a legal advisor before any further dissemination takes place; the retention or dissemination of legally privileged material should be accompanied by a clear warning that it is subject to legal privilege; it should be safeguarded by taking "reasonable steps" to ensure there is no possibility of it becoming available, or it contents becoming known, to any person whose possession of it might prejudice any criminal or civil proceedings; and finally, any dissemination to an outside body should be notified to the relevant Commissioner or Inspector during his next inspection.

139. These provisions, although containing some significant safeguards to protect the interests of persons affected by the surveillance of legal consultations, are to be contrasted with the more detailed provisions in Part I of RIPA and the Interception of Communications Code of Practice,

		which the Court approved in Kennedy (cited above, §§ 42 – 49). In particular, in relation to intercepted material there are provisions in Part I and the Code of Practice limiting the number of persons to whom the material is made available and restricting the extent to which it is disclosed and copied; imposing a broad duty on those involved in interception to keep everything in the intercepted material secret; prohibiting disclosure to persons who do not hold the necessary security clearance and to persons who do not "need to know" about the material; criminalising the disclosure of intercept material with an offence punishable by up to five years' imprisonment; requiring intercepted material to be stored securely; and requiring that intercepted material be securely destroyed as soon as it is no longer required for any of the authorised purposes. 140. Paragraph 9.3 of the Revised Code does provide that each public authority must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through directed or intrusive surveillance. In the present case the relevant arrangements are contained in the PSNI Service Procedure on Covert Surveillance of Legal Consultations and the Handling of Legally Privileged Material. The Administrative Court accepted that taking together the 2010 Order, the Revised Code and the PSNI Service Procedure Implementing Code, the arrangements in place for the use, retention and destruction of retained material in the context of legal consultations was compliant with the Article 8 rights of persons in custody. However, the Service Procedure was only implemented on 22 June 2010. It was therefore not in force during the applicant's detention in May 2010. 141. The Court has noted the statement of the Government in their observations that only one intrusive surveillance order had been granted up till then in the three years since the 2010 Order (introducing the Revised Code) had come into force in April 2010 (see paragraphs 11 and 12 above). Nevertheless, in the absence of the "arrangements" anticipated by the covert surveillance regime, the Court, sharing the concerns of Lord Phillips and Lord Neuberger in the House of Lords in this regard (see paragraphs 36 – 37 above) is not satisfied that the provisions in Part II of RIPA and the Revised Code concerning the examination, use and storage of the material obtained, the precautions to be taken when communicating the material to other parties, and the circumstances in which recordings may or must be erased or the material destroyed provide sufficient safeguards for the protection of the material obtained by covert surveillance.
63.	Eur. Court of HR., *Roman Zakharov v Russia* judgment of 4 December 2015, 47143/06: review of law in the abstract, secret surveillance measures, clarity of the law, safeguards against abuse, effective remedies	148. The applicant complained that the system of covert interception of mobile telephone communications in Russia did not comply with the requirements of Article 8 of the Convention 252. The Court concludes from the above that while Russian law contains clear rules on the duration and renewal of interceptions providing adequate safeguards against abuse, **the OSAA provisions on discontinuation of the surveillance measures do not provide sufficient guarantees against arbitrary interference.** **256. Furthermore, as regards the cases where the person has been charged with a criminal offence, the Court notes with concern that Russian law allows unlimited discretion to the trial judge to store or to destroy the data used in evidence after the end of the trial (see paragraph 66 above). Russian law does not give citizens any indication as to the circumstances in which the intercept material may be stored after the end of the trial. The Court therefore**

considers that the domestic law is not sufficiently clear on this point.

267. In view of the above considerations the Court considers that the authorisation procedures provided for by Russian law are not capable of ensuring that secret surveillance measures are not ordered haphazardly, irregularly or without due and proper consideration.

285. In view of the defects identified above, and taking into account the particular importance of supervision in a system where law-enforcement authorities have direct access to all communications, **the Court considers that the prosecutors' supervision of interceptions as it is currently organised is not capable of providing adequate and effective guarantees against abuse.**

300. In view of the above considerations, the Court finds that Russian law does not provide for effective remedies to a person who suspects that he or she has been subjected to secret surveillance. **By depriving the subject of interception of the effective possibility of challenging interceptions retrospectively, Russian law thus eschews an important safeguard against the improper use of secret surveillance measures.**

302. The Court concludes that Russian legal provisions governing interceptions of communications do not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which is inherent in any system of secret surveillance, and which is particularly high in a system where the secret services and the police have direct access, by technical means, to all mobile telephone communications. In particular, the circumstances in which public authorities are empowered to resort to secret surveillance measures are not defined with sufficient clarity. Provisions on discontinuation of secret surveillance measures do not provide sufficient guarantees against arbitrary interference. The domestic law permits automatic storage of clearly irrelevant data and **is not sufficiently clear as to the circumstances in which the intercept material will be stored and destroyed after the end of a trial. The authorisation procedures are not capable of ensuring that secret surveillance measures are ordered only when "necessary in a democratic society". The supervision of interceptions, as it is currently organised, does not comply with the requirements of independence, powers and competence which are sufficient to exercise an effective and continuous control, public scrutiny and effectiveness in practice. The effectiveness of the remedies is undermined by the absence of notification at any point of interceptions, or adequate access to documents relating to interceptions.**

303. It is significant that the shortcomings in the legal framework as identified above appear to have an impact on the actual operation of the system of secret surveillance which exists in Russia. **The Court is not convinced by the Government's assertion that all interceptions in Russia are performed lawfully on the basis of a proper judicial authorisation.** The examples submitted by the applicant in the domestic proceedings (see paragraph 12 above) and in the proceedings before the Court (see paragraph 197 above) indicate the existence of arbitrary and abusive surveillance practices, which appear to be due to the inadequate safeguards provided by law (see, for similar reasoning, Association for European Integration and Human Rights and Ekimdzhiev, cited above, § 92; and, by contrast, Klass and Others, cited above, § 59, and Kennedy, cited above, §§ 168 and 169).

		304. In view of the shortcomings identified above, the Court finds that Russian law does not meet the "quality of law" requirement and is incapable of keeping the "interference" to what is "necessary in a democratic society".
64.	Eur. Court of HR., *Szabó and Vissy v. Hungary* judgment of 12 January 2016, 37138/14: secret surveillance, safeguards, margin of appreciation, quality of the law, supervision, remedies	56. In its case-law on secret measures of surveillance, the Court has developed the following **minimum safeguards** that should be set out in law in order to avoid abuses of power: **the nature of offences which may give rise to an interception order; the definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed** (see Huvig v. France, 24 April 1990, § 34, Series A no. 176-B; Amann v. Switzerland [GC], no. 27798/95, §§ 56-58, ECHR 2000-11; Valenzuela Contreras v. Spain, 30 July 1998, § 46, Reports 1998-V; Prado Bugallo v. Spain, no. 58496/00, § 30, 18 February 2003; Weber and Saravia, cited above, § 95; Association for European Integration, cited above, § 76; and Roman Zakharov, cited above, § 231). 57. When balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, this margin is subject to European supervision embracing both legislation and decisions applying it. **In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse.** The assessment depends on all **the circumstances of the case**, such as **the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law.** The Court has to determine **whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society"** (see Klass and Others, cited above, §§ 49, 50 and 59; Weber and Saravia, cited above, §106; Kvasnica v. Slovakia, no. 72094/01, § 80, 9 June 2009; Kennedy, cited above, §§ 153 and 154; and Roman Zakharov, cited above, § 232). 58. The Court has found an interference under Article 8 § 1 in respect of the applicants' general complaint about the rules of "section 7/E (3) surveillance" and not in respect of any actual interception activity allegedly taking place. Accordingly, in its examination of the justification for the interference under Article 8 § 2, the Court is required to examine this legislation itself and the safeguards built into the system allowing for secret surveillance, rather than the proportionality of any specific measures taken in respect of the applicants. In the circumstances, the lawfulness of the interference is closely related to the question whether the "necessity" test has been complied with in respect of the "section 7/E (3) surveillance" regime and it is therefore appropriate for the Court to address jointly the "in accordance with the law" and "necessity" requirements (see Kvasnica, cited above, § 84). 62. The reference to "foreseeability" in the context of interception of communications cannot be the same as in many other fields.

Foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated. **The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures** (see Roman Zakharov, cited above, § 229).

67. It is of serious concern, however, that the notion of "persons concerned identified ... as a range of persons" might include indeed any person and be interpreted as paving the way for the unlimited surveillance of a large number of citizens. The Court notes the absence of any clarification in domestic legislation as to how this notion is to be applied in practice (see, mutatis mutandis, Roman Zakharov, cited above, § 245). For the Court, the category is overly broad, because **there is no requirement of any kind for the authorities to demonstrate the actual or presumed relation between the persons or range of persons "concerned" and the prevention of any terrorist threat – let alone in a manner enabling an analysis by the authoriser which would go to the question of strict necessity** (see in paragraphs 72 and 73 below) with regard to the aims pursued and the means employed – although such an analysis appears to be warranted by section 53 (2) of the National Security Act, according to which "secret intelligence gathering [may only be applied] if the intelligence needed ... cannot be obtained in any other way".

68. For the Court, it is a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies in pre-empting such attacks, including the massive monitoring of communications susceptible to containing indications of impending incidents. **The techniques applied in such monitoring operations have demonstrated a remarkable progress in recent years and reached a level of sophistication which is hardly conceivable for the average citizen (see the CDT's submissions on this point in paragraphs 49-50 above), especially when automated and systemic data collection is technically possible and becomes widespread. In the face of this progress the Court must scrutinise the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights.** These data often compile further information about the conditions in which the primary elements intercepted by the authorities were created, such as the time and place of, as well as the equipment used for, the creation of computer files, digital photographs, electronic and text messages and the like. **Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives.** In this context the Court also refers to the observations made by the Court of Justice of the European Union and, especially, the United Nations Special Rapporteur, **emphasising the importance of adequate legislation of sufficient**

safeguards in the face of the authorities' enhanced technical possibilities to intercept private information (see paragraphs 23 and 24 above).

73. However, given the particular character of the interference in question and the potential of cutting-edge surveillance technologies to invade citizens' privacy, **the Court considers that the requirement "necessary in a democratic society" must be interpreted in this context as requiring "strict necessity" in two aspects. A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation.** In the Court's view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal. The Court notes that both the Court of Justice of the European Union and the United Nations Special Rapporteur require secret surveillance measures to answer to strict necessity (see paragraphs 23 and 24 above) – an approach it considers convenient to endorse. Moreover, particularly in this context the Court notes the absence of prior judicial authorisation for interceptions, the importance of which will be examined below in paragraphs 75 et seq. This safeguard would serve to limit the law-enforcement authorities' discretion in interpreting the broad terms of "persons concerned identified ... as a range of persons" by following an established judicial interpretation of the terms or an established practice to verify whether sufficient reasons for intercepting a specific individual's communications exist in each case (see, mutatis mutandis, Roman Zakharov, cited above, § 249). It is only in this way that the need for safeguards to ensure that emergency measures are used sparingly and only in duly justified cases can be satisfied (see Roman Zakharov, cited above, § 266).

74. Furthermore, in respect of the duration of any surveillance, the National Security Act stipulates, first, the period after which a surveillance permission will expire (that is, after a maximum of 90 days, as per section 58 (4) of the National Security Act) and, second, the conditions under which a renewal is possible. Permissions can be renewed for another 90 days; and the government minister in charge must authorise any such renewal upon a reasoned proposal from the service involved (see paragraph 17 above). Section 60 stipulates that the permission must be cancelled if it is no longer necessary, if the continued surveillance has no prospect of producing results, if its time-limit has expired or if it turns out to be in breach of the law for any reason. **The Court cannot overlook, however, that it is not clear from the wording of the law – especially in the absence of judicial interpretation – if such a renewal of the surveillance warrant is possible only once or repeatedly, which is another element prone to abuse.**

75. A central issue common to both the stage of authorisation of surveillance measures and the one of their application is the absence of judicial supervision. The measures are authorised by the Minister in charge of justice upon a proposal from the executives of the relevant security services, that is, of the TEK which, for its part, is a dedicated tactical department within the police force, subordinated to the Ministry of Home Affairs, with extensive prerogatives to apply force in combating terrorism (see section 1(2) subsection 15 of the Police Act quoted in paragraph 16 above). For the Court, this supervision, eminently political (as observed by the Constitutional Court, see point 105 of the decision quoted in paragraph 20 above) but carried out by the Minister of Justice

who appears to be formally independent of both the TEK and of the Minister of Home Affairs – is inherently incapable of ensuring the requisite assessment of strict necessity with regard to the aims and the means at stake. In particular, although the security services are required, in their applications to the Minister for warrants, to outline the necessity as such of secret information gathering, **this procedure does not guarantee that an assessment of strict necessity is carried out, notably in terms of the range of persons and the premises concerned** (see section 57 (2) of the National Security Act quoted in paragraph 17 above).

77. As regards the authority competent to authorise the surveillance, authorising of telephone tapping by a non-judicial authority may be compatible with the Convention (see, for example, Klass and Others, cited above, § 51; Weber and Saravia, cited above, § 115; and Kennedy, cited above, § 31), provided that that authority is sufficiently independent from the executive (see Roman Zakharov, cited above, § 258). However, the political nature of the authorisation and supervision increases the risk of abusive measures. The Court recalls that the rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure. (…)

78. The governments' more and more widespread practice of transferring and sharing amongst themselves intelligence retrieved by virtue of secret surveillance – a practice, whose usefulness in combating international terrorism is, once again, not open to question and which concerns both exchanges between Member States of the Council of Europe and with other jurisdictions – is yet another factor in requiring particular attention when it comes to external supervision and remedial measures.

79. It is in this context that the external, preferably judicial, a posteriori control of secret surveillance activities, both in individual cases and as general supervision, gains its true importance (see also Klass and Others, cited above, §§ 56, 70 and 71; Dumitru Popescu, cited above, § 77; and Kennedy, cited above, §§ 184-191), by reinforcing citizens' trust that guarantees of the rule of law are at work even in this sensitive field and by providing redress for any abuse sustained. The significance of this control cannot be overestimated in view of the magnitude of the pool of information retrievable by the authorities applying highly efficient methods and processing masses of data, potentially about each person, should he be, one way or another, connected to suspected subjects or objects of planned terrorist attacks. **The Court notes the lack of such a control mechanism in Hungary.**

81. Furthermore, where situations of extreme urgency are concerned, the law contains a provision under which the director of the service may himself authorise secret surveillance measures for a maximum of 72 hours (see sections 58 and 59 of the National Security Act quoted in paragraph 17 above). For the Court, this exceptional power should be sufficient to address any situations in which external, judicial control would run the risk of losing precious time. Such measures must however be subject to a post factum review, which is required, as a rule, in cases where the surveillance was authorised ex ante by a non-judicial authority.

82. The Court notes at this juncture the liability of the executive to give account, in general terms rather than concerning any individual cases, of

such operations to a parliamentary committee. **However, it cannot identify any provisions in Hungarian legislation permitting a remedy granted by this procedure during the application of measures of secret surveillance to those who are subjected to secret surveillance but, by necessity, are kept unaware thereof.** The Minister is under an obligation to present a general report, at least twice a year, to the responsible parliamentary committee about the functioning of national security services, which report, however, does not seem to be available to the public and by this appears to fall short of securing adequate safeguards in terms of public scrutiny (see Roman Zakharov, cited above, § 283). The committee is entitled, of its own motion, to request information from the Minister and the directors of the services about the activities of the national security services. However, the Court is not persuaded that this scrutiny is able to provide redress to any individual grievances caused by secret surveillance or to control effectively, that is, in a manner with a bearing on the operations themselves, the daily functioning of the surveillance organs, especially since it does not appear that the committee has access in detail to relevant documents. **The scope of their supervision is therefore limited** (see, mutatis mutandis, Roman Zakharov, cited above, § 281).

83. Moreover, the complaint procedure outlined in section 11(5) of the National Security Act seems to be of little relevance, since citizens subjected to secret surveillance will not take cognisance of the measures applied. In regard to the latter point, the Court shares the view of the Venice Commission according to which "individuals who allege wrongdoing by the State in other fields routinely have a right of action for damages before the courts. The effectiveness of this right depends, however, on the knowledge of the individual of the alleged wrongful act, and proof to the satisfaction of the courts." (see point 243 of the Report, quoted in paragraph 21 above). A complaint under section 11(5) of the National Security Act will be investigated by the Minister of Home Affairs, who does not appear to be sufficiently independent (see Association for European Integration, cited above, § 87; and Roman Zakharov, cited above, § 278).

84. The Court further notes the evidence furnished by the applicants according to which the Commissioner for Fundamental Rights has never so far enquired into the question of secret surveillance (see paragraph 18 above).

85. In any event, the Court recalls that in Klass and Others a combination of oversight mechanisms, short of formal judicial control, was found acceptable in particular because of "an initial control effected by an official qualified for judicial office" (cited above, § 56). However, the Hungarian scheme of authorisation does not involve any such official. The Hungarian Commissioner for Fundamental Rights has not been demonstrated to be a person who necessarily holds or has held a judicial office (see, a contrario, Kennedy, cited above, § 57).

86. Moreover, the Court has held that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for any recourse by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their justification retrospectively. As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should be provided to the

		persons concerned (see Weber and Saravia, cited above, §135; Roman Zakharov, cited above, § 287). In Hungarian law, however, no notification, of any kind, of the measures is foreseen. This fact, coupled with the absence of any formal remedies in case of abuse, indicates that the legislation falls short of securing adequate safeguards. 87. It should be added that although the Constitutional Court held that various provisions in the domestic law read in conjunction secured sufficient safeguards for data storage, processing and deletion, special reference was made to the importance of individual complaints made in this context (see point 138 of the decision, quoted in paragraph 20 above). **For the Court, the latter procedure is hardly conceivable, since once more it transpires from the legislation that the persons concerned will not be notified of the application of secret surveillance to them.** **88. Lastly, the Court notes that is for the Government to illustrate the practical effectiveness of the supervision arrangements with appropriate examples** (see Roman Zakharov, cited above, § 284). **However, the Government were not able to do so in the instant case.**
65.	*Figueiredo Teixeira v. Andorra* judgment of 8 November 2016, 72384/14: secret surveillance/telephone surveillance, safeguards	41. La Cour rappelle en outre que la précision requise de la législation interne – laquelle ne peut en aucun cas prévoir toutes les hypothèses – dépend dans une large mesure du contenu de l'instrument en question, du domaine qu'il est censé couvrir ainsi que du nombre et de la qualité de ceux à qui il s'adresse (voir Hassan et Tchaouch c. Bulgarie [GC], no 30985/96, § 84, CEDH 2000-XI, et les affaires qui y sont citées). 42. En l'espèce, la Cour constate que l'article 87 du code de procédure pénale en vigueur au moment des faits énonçait de façon détaillée les conditions dans lesquelles l'ingérence dans le droit à la vie privée était autorisée (voir, a contrario, Rotaru, précité, §§ 57-63). En particulier, l'article 87 § 5 prévoyait que le juge devait rendre une décision motivée, en prenant compte de la nécessité de la mesure ainsi que de sa proportionnalité, eu égard aux indices obtenus et à la gravité du délit objet de l'enquête. La Cour considère que l'ordonnance du 30 août 2012 respectait ces exigences, compte tenu, notamment, des besoins de l'instruction, de la gravité du délit sous-jacent (trafic de drogue) et des modalités pratiques de l'intrusion dans la sphère privée du requérant. 43. En cela, la présente affaire diffère de l'affaire Malone (précitée), invoquée par le requérant, dans laquelle la Cour a conclu à la violation de l'article 8 de la Convention. La Cour rappelle que, comme le Tribunal constitutionnel andorran l'a indiqué dans son arrêt du 13 mars 2014, elle a estimé dans son arrêt Malone (précité) que la pratique consistant à transmettre les données obtenues au moyen d'un système de « comptage » ne soulevait pas, en tant que telle, de problème à l'égard de la Convention, et que ce qui posait problème était la transmission de ces données directement à la demande d'un service de police, d'une autorité administrative ou d'un ministre. **Force est de constater en l'espèce que la procédure andorrane offre des nombreuses garanties contre les comportements arbitraires : a) c'est toujours un juge (Batlle) qui autorise, en amont, la mesure, b) la durée maximale de cette dernière est fixée par la loi et intéresse seulement les délits les plus graves et c) le requérant peut toujours contester la légalité de la preuve obtenue au cours du procès, conformément à l'article 9 § 3 de la Loi qualifiée sur la justice.** 44. En l'espèce, la Cour souligne que, dans son article 5, la loi qualifiée no 15/2003 exclut clairement de son champ d'application le traitement des

		données liées à la prévention des infractions pénales. Dans le même sens, l'article 16 prévoit que la communication de données personnelles à la suite d'une décision de justice ne peut pas faire l'objet d'une opposition de la part de la personne concernée. 45. En ce qui concerne la réglementation portant sur la téléphonie mobile, la Cour note que le décret du 18 mars 2009, relatif aux fichiers de données personnelles « clients », « clients potentiels », « contrôle d'accès », « gestion de ressources humaines », « sélection de personnel » et « tiers et fournisseurs » de Andorra Telecom, qui vient en complément de la loi qualifiée no 15/2003 susmentionnée, précise, dans ses annexes, les modalités de stockage des données des clients ainsi que la procédure à suivre en cas de demande de rectification ou d'opposition. 46. Reste à savoir si le requérant, détenteur d'une carte prépayée, pouvait s'attendre à se voir appliquer toutes ces normes concurrentes. À cet égard, la Cour signale que les règles susmentionnées ne distinguent pas les titulaires d'un contrat de téléphonie mobile des utilisateurs d'une carte prépayée. Il est raisonnable de considérer, à l'instar des arguments formulés par le ministère public dans le recours d'empara et repris par le Tribunal constitutionnel, que ces textes sont applicables aux deux types de services de téléphonie. **47. À la lumière de ce qui précède, la Cour considère que l'application du droit interne au cas d'espèce était suffisamment prévisible au sens de l'article 8 § 2 de la Convention** (voir, a contrario, Dragojević c. Croatie, no 68955/11, § 101, 15 janvier 2015). **49. Quant au caractère proportionné de la mesure, la Cour signale que l'ingérence litigieuse a été autorisée pour une période inférieure à celle que le service de police avait demandée dans son rapport du 5 décembre 2011.** De plus, les faits reprochés n'étaient pas antérieurs de plus de six mois à la période visée par la mesure litigieuse. 50. Se référant en outre à la Recommandation Rec (2005) 10 du Comité des Ministres du Conseil de l'Europe aux États membres, relative aux techniques spéciales d'enquête en relation avec des infractions graves, adoptée le 20 avril 2005, la Cour est d'avis que les autorités andorranes ont respecté la « proportionnalité entre les conséquences de l'utilisation des techniques spéciales d'enquête et le but qui a été identifié », et qu'elles ont usé d'une méthode peu intrusive afin « de découvrir l'infraction, de la prévenir ou d'en poursuivre l'auteur, avec une efficacité adéquate ». En effet, le juge aurait pu prendre des mesures plus intrusives, affectant la vie privée du requérant, par exemple soumettre l'intéressé à une prise de sang afin de vérifier son argument selon lequel les substances trouvées étaient destinées à sa consommation personnelle et non à la vente. **51. Il s'ensuit que, dans la présente espèce, l'équilibre entre le droit à la vie privée du requérant et la prévention des infractions pénales a été respecté.**
66.	*Dimitar Vasilev v Bulgaria*, 10.04.2012, Application no. 10302/05: prisoner's correspondence surveillance with lawyer	48. The Court notes that the systematic opening of the applicant's letters was acknowledged by the Government in their observations in the present case (see paragraph 45 above). It further notes that it has frequently found violations of Article 8 of the Convention in Bulgarian cases concerning indiscriminate opening by the authorities of prisoners' correspondence with their lawyers (see, among many others, Radkov v. Bulgaria, no. 27795/03, §§ 20-22, 22 April 2010, and Konstantin Popov v. Bulgaria, no. 15035/03, § 17, 25 June 2009).

		49. It has also found that the monitoring of prisoners' correspondence had not resulted from one individual decision taken by the authorities but directly from the application of the relevant legislation in the relevant period. However, it has concluded that there was no violation of Article 13 of the Convention because this provision does not guarantee a remedy allowing a Contracting State's primary legislation to be challenged before a national authority (see Konstantin Popov, § 23, cited above, and Petrov v. Bulgaria, no. 15197/02, § 65, 22 May 2008). 50. Having examined all the material submitted to it, the Court considers that the Government have not put forward any fact or argument capable of persuading it to reach different conclusions in the present case. There has therefore been a violation of Article 8 and no violation of Article 13 of the Convention.
67.	*Modestou c. Grece*, Requête no 51693/13, 16 mars 2017: police search, judicial control	51. La Cour constate que le requérant n'était présent à aucun moment de la perquisition, laquelle a duré douze heures et demie, et que le dossier ne permet pas de savoir si les enquêteurs ont tenté de l'informer de leur présence ou de leur action, alors que l'article 256 du CPP fait obligation à celui qui mène la perquisition d'inviter l'occupant des lieux à être présent. À supposer même que les autorités aient voulu obtenir un effet de surprise en évitant de prévenir à l'avance le requérant, rien ne les empêchaient, afin de se conformer à la lettre de l'article précité, de chercher à prendre contact avec lui pendant le déroulement de la perquisition en question qui s'est prolongée sur quelques heures. Quant à la voisine néerlandaise que les enquêteurs ont appelée pour qu'elle agît comme témoin, le Gouvernement n'a pas démontré qu'elle avait une maîtrise de la langue grecque lui permettant de recevoir des informations suffisantes sur les poursuites à l'origine de l'opération ou sur la nature des objets et documents recherchés. 52. À l'absence d'un contrôle judiciaire ex ante, à l'imprécision du mandat et à l'absence physique du requérant, se rajoute l'absence d'un contrôle judiciaire ex post factum immédiat. En effet, la perquisition a abouti à la saisie de deux ordinateurs et de centaines des documents dont il n'a jamais été élucidé si tous avaient un rapport direct avec l'infraction sous examen. Au vu du texte du mandat, l'on peut aussi se demander si le requérant avait été informé du cadre dans lequel la perquisition s'inscrivait, ce qui lui aurait permis de vérifier que la perquisition se limitait à la recherche de l'infraction mentionnée dans le mandat et d'en dénoncer d'éventuels abus (voir, mutatis mutandis, Van Rossem, précité, § 48). La chambre d'accusation de la cour d'appel d'Athènes, saisie par le requérant, a rendu sa décision plus de deux ans après la perquisition en question et a consacré la plus grande partie de sa décision à la question de savoir s'il était possible de procéder à une perquisition et à une saisie dans le cadre d'une enquête préliminaire. Les autorités internes ont donc manqué à l'obligation qu'elles avaient de justifier par des motifs « pertinents et suffisants » l'émission du mandat de perquisition (voir aussi Smirnov, précité, § 47). **53. Ces éléments suffisent à la Cour pour conclure à l'absence de proportionnalité de l'ingérence avec le but poursuivi. Cela la dispense par ailleurs d'examiner les autres allégations du requérant, notamment celles relatives à l'absence, lors de la perquisition, de témoins ayant des connaissances juridiques et aux conséquences de la perquisition sur la confidentialité des données professionnelles du requérant.** 54. La Cour estime dès lors que le Gouvernement n'a pas démontré qu'une

		balance équitable des intérêts en présence a été préservée en l'espèce. Elle en conclut que les mesures litigieuses ne représentaient pas des moyens raisonnablement proportionnés à la poursuite des buts légitimes visés compte tenu de l'intérêt de la société démocratique à assurer le respect du domicile. Il y a donc eu violation de l'article 8 de la Convention.
68.	*Porowski v. Poland*, Application no. 34458/03, 21 March 2017: rights of detainees, communication with lawyer	169. The Court notes that the interference occurred while the applicant was in detention on remand and that the Government have failed to show that it had any legal basis in domestic law. **170. The Court observes that under Article 214 of the Code of Execution of Criminal Sentences, detainees enjoy the same rights as those convicted by a final judgment. Accordingly, the prohibition on censorship of correspondence with a detainee's counsel contained in Article 8 § 3 of the same Code, which expressly relates to convicted people, is also applicable to prisoners on remand** (see Michta, cited above, § 61, and Kwiek v. Poland, no. 51895/99, § 44, 30 May 2006). Moreover, the prohibition on censorship of convicted people's correspondence with the Court, which is set forth in Article 103 of the Code of Execution of Criminal Sentences, is likewise applicable to those remanded in custody (for domestic provisions concerning monitoring of detainees' correspondence, (see paragraph 89 above). 171. The censorship of the applicant's letters to his lawyer and to the Court was therefore contrary to domestic law. It follows that the interference in the present case was not "in accordance with the law".
69.	*Draksas v Lithaunia*, Application no. 36662/04, 31 July 2012: Disclosure of telephone conversations to the media by police, (not) in accordance with the law	59. Turning to the matter of the disclosure of the applicant's telephone conversations, the Court notes that the applicant complained about two separate sets of facts, namely the disclosure of his telephone conversation of 16 March 2003 with a Russian businessman, J.B., and the disclosure of his conversations with his business partners and the State President while the impeachment proceedings were pending before the Constitutional Court. The Court will analyse each of these issues separately. 60. The Court notes that on 2 November 2003 the recorded conversation between the applicant and J.B. was aired on two Lithuanian television channels. Even though the recording had been declassified a day earlier by the SSD, it is the Court's view that the recording still ought to have been kept confidential from the general public. **As appears from the SSD's letter, at that time the Attorney General's Office was examining the recording in the framework of criminal proceedings, and, pursuant to Article 177 of the Code of Criminal Procedure, information about the pre-trial investigation had to remain confidential.** Nonetheless, the conversation became known to the public. The fact that the SSD had exploited the information was also confirmed by the prosecutor on 11 November 2003 (paragraphs 14 and 15 above). **The Court thus concludes that despite the legal provisions designed to ensure that the surveillance is carried out in strict accordance with the law in order to protect a person's privacy against abuse, the actual practice followed in this case was different.** Whilst acknowledging the Government's argument that the public had a right to information about one of its civil servants, the Court nevertheless considers that the SSD was responsible for keeping the information confidential. Lastly, the Court cannot fail to observe that to this day the Lithuanian authorities have not discovered who leaked the conversation to the media (paragraphs 35 and 36 above). **In these circumstances, the Court concludes that the lack of protection exercised in respect of the applicant's telephone conversation with J.B. was not in accordance with the law. This gives rise to a violation of Article 8 of the Convention.**

70.	*G.S.B. v Switzerland*, Application no. 28601/11, 22 December 2015: mutual assistance with a Third State – preliminary criminal proceedings - safeguards	78. In the present case the Federal Court has constant case-law to the effect that the provisions on administrative and criminal mutual assistance requiring third parties to provide specific types of information are of a procedural nature and therefore apply, in principle, to all proceedings that are under way or are forthcoming, even where they concern tax years preceding their enactment ... 93. As regards the applicant's private interests, it transpires from the aforementioned case-law that the protection afforded to personal data depends on a number of factors, including the nature of the relevant Convention right, its importance to the person in question, and the nature and purpose of the interference. According to the S. and Marper judgment (cited above, § 102), a State's margin of appreciation will tend to be narrower where the right at stake is crucial to the individual's effective enjoyment of intimate or key rights. Where a particularly important facet of an individual's existence or identity is at stake, the margin allowed to the State will be restricted. **As regards the applicant's situation, it should be noted that the impugned disclosure only concerned his bank data, that is to say purely financial information; it therefore in no way involved the transmission of intimate details or data closely linked to his identity, which would have merited enhanced protection. It follows that Switzerland had a broad margin of appreciation in his case.** 94. With reference to its observations on the pursuit of a legitimate aim (see paragraphs 83 and 84 above), the Court accepts that **Switzerland had an important interest in acceding to the American request for administrative mutual assistance so that the US could track down any assets concealed in Switzerland.** By concluding Agreement 09 and Protocol 10, it succeeded in averting a major conflict with the United States of America. **95. As regards the effect of the impugned measure on the applicant, the Court once again observes that the measure was implemented in the framework of a mutual assistance procedure, not as part of any criminal proceedings conducted in the USA, which were, and still are, purely hypothetical, and that that procedure represents at most a mere preliminary phase to criminal proceedings.** In other words, the bank details in question were transmitted to the competent US authorities to enable them to assess, using their standard procedures, whether the applicant had indeed honoured his tax obligations, and if not, to take the requisite legal action. **96. The Court also observes that the applicant benefited from certain procedural safeguards against the transfer of his data to the US tax authorities** (see, conversely, M.N. and Others v. San Marino, cited above, §§ 82 et seq.). Firstly, he was able to appeal to the Federal Administrative Court against the AFC's decision of 7 June 2010 (see paragraph 20 above). That court subsequently set aside the said decision owing to a breach of the applicant's right to a hearing. The AFC consequently invited the applicant to transmit any observations he might have within a specified time-limit. The applicant availed himself of that right. On 4 November 2010 the AFC gave a fresh decision, which was properly reasoned, reaching the conclusion that all the preconditions were present for affording administrative mutual assistance. Subsequently, the applicant lodged a second appeal with the Federal Administrative Court, which dismissed that appeal by judgment of 2 March 2011 (see paragraphs 21

		and 22 above). It follows that the applicant had several effective and real procedural safeguards at his disposal to challenge the surrender of his bank details, thereby protecting him against arbitrary implementation of the agreements concluded by Switzerland and the United States of America. 97. Having regard to all the circumstances of the case, and particularly in the light of the non-personal nature of the data disclosed, it was not unreasonable for Switzerland to prioritise the general interest of an effective and satisfactory settlement with the United States of America over the private interest of the applicant. That being the case, Switzerland did not overstep its margin of appreciation.
Nr	**CJEU Judgement/Opinion**	Paragraph/Text
1	C – 293/12 und C-594/12, *Digital Rights Ireland*, 8 April 2014: storage of electronic communication data for law-enforcement purposes, proportionality, safeguards	29 The retention of data for the purpose of possible access to them by the competent national authorities, as provided for by Directive 2006/24, directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 of the Charter. Furthermore, such a retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, therefore, necessarily has to satisfy the data protection requirements arising from that article (Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert EU:C:2010:662, paragraph 47). 30 Whereas the references for a preliminary ruling in the present cases raise, in particular, the question of principle as to whether or not, in the light of Article 7 of the Charter, the data of subscribers and registered users may be retained, they also concern the question of principle as to whether Directive 2006/24 meets the requirements for the protection of personal data arising from Article 8 of the Charter. 31 In the light of the foregoing considerations, it is appropriate, for the purposes of answering the second question, parts (b) to (d), in Case C-293/12 and the first question in Case C-594/12, to examine the validity of the directive in the light of Articles 7 and 8 of the Charter. On the existence of interference: 34 As a result, the obligation imposed by Articles 3 and 6 of Directive 2006/24 on providers of publicly available electronic communications services or of public communications networks **to retain, for a certain period, data relating to a person's private life and to his communications, such as those referred to in Article 5 of the directive, constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter.** **35 Furthermore, the access of the competent national authorities to the data constitutes a further interference with that fundamental right** (see, as regards Article 8 of the ECHR, Eur. Court H.R., Leander v. Sweden, 26 March 1987, § 48, Series A no 116; Rotaru v. Romania [GC], no. 28341/95, § 46, ECHR 2000-V; and Weber and Saravia v. Germany (dec.), no. 54934/00, § 79, ECHR 2006-XI). Accordingly, Articles 4 and 8 of Directive 2006/24 laying down rules relating to the access of the competent national authorities to the data also constitute an interference with the rights guaranteed by Article 7 of the Charter. **36 Likewise, Directive 2006/24 constitutes an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter because it provides for the processing of personal data.**

37 It must be stated that the interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is, as the Advocate General has also pointed out, in particular, in paragraphs 77 and 80 of his Opinion, wide-ranging, and it must be considered to be particularly serious. Furthermore, as the Advocate General has pointed out in paragraphs 52 and 72 of his Opinion, **the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.**

On the justification for the interference:
- Legitimate purpose and essence of the right criteria fulfilled (pars. 38-44).

48 In the present case, in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict.

49 As regards the question of whether the retention of data is appropriate for attaining the objective pursued by Directive 2006/24, it must be held that, having regard to the growing importance of means of electronic communication, data which must be retained pursuant to that directive allow the national authorities which are competent for criminal prosecutions to have additional opportunities to shed light on serious crime and, in this respect, they are therefore a valuable tool for criminal investigations. Consequently, the retention of such data may be considered to be appropriate for attaining the objective pursued by that directive.

52 So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply **only in so far as is strictly necessary** (Case C‑473/12 IPI EU:C:2013:715, paragraph 39 and the case-law cited).

53 In that regard, it should be noted that the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter.

54 Consequently, the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data (see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., Liberty and Others v. the United Kingdom, 1 July 2008, no. 58243/00, § 62 and 63; Rotaru v. Romania, § 57 to 59, and S. and Marper v. the United Kingdom, § 99).

55 **The need for such safeguards is all the greater where, as laid down in Directive 2006/24, personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data** (see, by analogy, as regards Article 8 of the ECHR, S. and Marper v. the United Kingdom, § 103, and M. K. v. France, 18 April 2013, no. 19522/09, § 35).

56 As for the question of whether the interference caused by Directive 2006/24 is limited to what is strictly necessary, it should be observed that, in accordance with Article 3 read in conjunction with Article 5(1) of that directive, the directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony. **It therefore applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. Furthermore, in accordance with Article 3 of Directive 2006/24, the directive covers all subscribers and registered users. It therefore entails an interference with the fundamental rights of practically the entire European population.**

57 **In this respect, it must be noted, first, that Directive 2006/24 covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.**

58 Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. **It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.**

59 Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 **does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.**

60 Secondly, not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also **fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference**. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law.

61 Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of

preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements.

62 In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.

63 Thirdly, so far as concerns the data retention period, Article 6 of Directive 2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.

64 Furthermore, that **period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.**

65 It follows from the above that Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.

66 Moreover, as far as concerns the rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks, it must be held that Directive 2006/24 **does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data.** In the first place, Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.

67 Article 7 of Directive 2006/24, read in conjunction with Article 4(1) of Directive 2002/58 and the second subparagraph of Article 17(1) of

		Directive 95/46, does not ensure that a particularly high level of protection and security is applied by those providers by means of technical and organisational measures, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures. In particular, Directive 2006/24 does not ensure the irreversible destruction of the data at the end of the data retention period. **68 In the second place, it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data** (see, to that effect, Case C-614/10 Commission v Austria EU:C:2012:631, paragraph 37). 69 Having regard to all the foregoing considerations, it must be held that, by adopting Directive 2006/24, **the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter.**
2.	C - 362/14, *Schrems*, 6.10.2015: re-use of data transferred to a Third Courtry for law-enforcement and security purposes, remedies, safegauards	86 Thus, Decision 2000/520 lays down that 'national security, public interest, or law enforcement requirements' have primacy over the safe harbour principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them. 87 In the light of the general nature of the derogation set out in the fourth paragraph of Annex I to Decision 2000/520, that decision thus enables interference, founded on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States. **To establish the existence of an interference with the fundamental right to respect for private life, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference** (judgment in Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraph 33 and the case-law cited). **88 In addition, Decision 2000/520 does not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security.** 89 Nor does Decision 2000/520 refer to the existence of effective legal protection against interference of that kind. As the Advocate General has observed in points 204 to 206 of his Opinion, **procedures before the Federal Trade Commission** — the powers of which, described in particular in FAQ 11 set out in Annex II to that decision, are limited to commercial disputes — and the private dispute resolution mechanisms

concern compliance by the United States undertakings with the safe harbour principles and **cannot be applied in disputes relating to the legality of interference with fundamental rights that results from measures originating from the State.**

90 Moreover, the foregoing analysis of Decision 2000/520 is borne out by the Commission's own assessment of the situation resulting from the implementation of that decision. Particularly in points 2 and 3.2 of Communication COM(2013) 846 final and in points 7.1, 7.2 and 8 of Communication COM(2013) 847 final, the content of which is set out in paragraphs 13 to 16 and paragraphs 22, 23 and 25 of the present judgment respectively**, the Commission found that the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security. Also, the Commission noted that the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased.**

91 As regards the level of protection of fundamental rights and freedoms that is guaranteed within the European Union, **EU legislation involving interference with the fundamental rights** guaranteed by Articles 7 and 8 of the Charter **must**, according to the Court's settled case-law**, lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data. The need for such safeguards is all the greater where personal data is subjected to automatic processing and where there is a significant risk of unlawful access to that data** (judgment in Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 54 and 55 and the case-law cited).

92 Furthermore and above all, protection of the fundamental right to respect for private life at EU level requires **derogations and** limitations in relation to the protection of personal data to apply **only in so far as is strictly necessary** (judgment in Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraph 52 and the case-law cited).

93 Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail (see, to this effect, concerning Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54), judgment in Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 57 to 61).

		94 In particular, **legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter** (see, to this effect, judgment in Digital Rights Ireland and Others, C‑293/12 and C‑594/12, EU:C:2014:238, paragraph 39). **95 Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.** The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law (see, to this effect, judgments in Les Verts v Parliament, 294/83, EU:C:1986:166, paragraph 23; Johnston, 222/84, EU:C:1986:206, paragraphs 18 and 19; Heylens and Others, 222/86, EU:C:1987:442, paragraph 14; and UGT-Rioja and Others, C‑428/06 to C‑434/06, EU:C:2008:488, paragraph 80).
3.	Joined Cases C‑203/15 and C‑698/15, *Tele2 Svergie*, 21.12.2016: e-Privacy, targeterd vs non-targeted retention of telecommunications data	93 **Accordingly, the importance both of the right to privacy, guaranteed in Article 7 of the Charter, and of the right to protection of personal data**, guaranteed in Article 8 of the Charter, as derived from the Court's case-law (see, to that effect, judgment of 6 October 2015, Schrems, C‑362/14, EU:C:2015:650, paragraph 39 and the case-law cited), **must be taken into consideration in interpreting Article 15(1) of Directive 2002/58. The same is true of the right to freedom of expression in the light of the particular importance accorded to that freedom in any democratic society.** That fundamental right, guaranteed in Article 11 of the Charter, constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the Union is founded (see, to that effect, judgments of 12 June 2003, Schmidberger, C‑112/00, EU:C:2003:333, paragraph 79, and of 6 September 2011, Patriciello, C‑163/10, EU:C:2011:543, paragraph 31). 97 As regards whether national legislation, such as that at issue in Case C‑203/15, satisfies those conditions, it must be observed that that legislation provides for a general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication, and that it imposes on providers of electronic communications services an obligation to retain that data systematically and continuously, with no exceptions. As stated in the order for reference, the categories of data covered by that legislation correspond, in essence, to the data whose retention was required by Directive 2006/24. 98 The data which providers of electronic communications services must therefore retain makes it possible to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to establish the location of mobile communication equipment. That data includes, inter alia, the name and address of the subscriber or registered user, the telephone number of the caller, the number called and an IP address for internet services. That data makes it possible, in particular, to identify the person with whom a subscriber or

registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. Further, that data makes it possible to know how often the subscriber or registered user communicated with certain persons in a given period (see, by analogy, with respect to Directive 2006/24, the Digital Rights judgment, paragraph 26).

99 That data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 27). In particular, that data provides the means, as observed by the Advocate General in points 253, 254 and 257 to 259 of his Opinion, **of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications.**

100 ... The fact that the data is retained without the subscriber or registered user being informed is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 37).

101 Even if such legislation does not permit retention of the content of a communication and is not, therefore, such as to affect adversely the essence of those rights (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 39), **the retention of traffic and location data could nonetheless have an effect on the use of means of electronic communication and, consequently, on the exercise by the users thereof of their freedom of expression, guaranteed in Article 11 of the Charter** (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 28).

102 Given the seriousness of the interference in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data, **only the objective of fighting serious crime is capable of justifying such a measure** (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 60).

103 **Further, while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight** (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 51).

104 In that regard, it must be observed, first, that the effect of such legislation, in the light of its characteristic features as described in paragraph 97 of the present judgment, is that the retention of traffic and location data is the rule, **whereas the system put in place by Directive 2002/58 requires the retention of data to be the exception.**

108 However, **Article 15(1) of Directive 2002/58, read in the light of**

Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.

109 In order to satisfy the requirements set out in the preceding paragraph of the present judgment, that national legislation must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. **That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary** (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 54 and the case-law cited).

110 Second, as regards the substantive conditions which must be satisfied by national legislation that authorises, in the context of fighting crime, the retention, as a preventive measure, of traffic and location data, if it is to be ensured that data retention is limited to what is strictly necessary, it must be observed that, while those conditions may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, **the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected.**

111 As regard the setting of limits on such a measure with respect to the public and the situations that may potentially be affected, **the national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security.** Such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences.

112 Having regard to all of the foregoing, the answer to the first question referred in Case C-203/15 is that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, **must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.**

115 As regards objectives that are capable of justifying national legislation that derogates from the principle of confidentiality of electronic communications, it must be borne in mind that, since, as stated in paragraphs 90 and 102 of this judgment, the list of objectives set out in the first sentence of Article 15(1) of Directive 2002/58 is exhaustive, access to the retained data must correspond, genuinely and strictly, to one of those

objectives. Further, since the objective pursued by that legislation must be proportionate to the seriousness of the interference in fundamental rights that that access entails, it follows that, in the area of prevention, investigation, detection and prosecution of criminal offences, **only the objective of fighting serious crime is capable of justifying such access to the retained data.**

116 As regards compatibility with the principle of proportionality, national legislation governing the conditions under which the providers of electronic communications services must grant the competent national authorities access to the retained data must ensure, in accordance with what was stated in paragraphs 95 and 96 of this judgment, that such access does not exceed the limits of what is strictly necessary.

117 Further, since the legislative measures referred to in Article 15(1) of Directive 2002/58 must, in accordance with recital 11 of that directive, 'be subject to adequate safeguards', a **data retention measure must**, as follows from the case-law cited in paragraph 109 of this judgment, **lay down clear and precise rules indicating in what circumstances and under which conditions the providers of electronic communications services must grant the competent national authorities access to the data. Likewise, a measure of that kind must be legally binding under domestic law.**

118 In order to ensure that access of the competent national authorities to retained data is limited to what is strictly necessary, it is, indeed, for national law to determine the conditions under which the providers of electronic communications services must grant such access. However, the national legislation concerned cannot be limited to requiring that access should be for one of the objectives referred to in Article 15(1) of Directive 2002/58, even if that objective is to fight serious crime. **That national legislation must also lay down the substantive and procedural conditions governing the access of the competent national authorities to the retained data** (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 61).

119 Accordingly, and since general access to all retained data, regardless of whether there is any link, at least indirect, with the intended purpose, cannot be regarded as limited to what is strictly necessary, the national legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data of subscribers or registered users. In that regard, access can, as a general rule, be granted, **in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime** (see, by analogy, ECtHR, 4 December 2015, Zakharov v. Russia, CE:ECHR:2015:1204JUD004714306, § 260). However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities.

120 In order to ensure, in practice, that those conditions are fully respected, it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, **be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned**

		request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 62; see also, by analogy, in relation to Article 8 of the ECHR, ECtHR, 12 January 2016, Szabó and Vissy v. Hungary, CE:ECHR:2016:0112JUD003713814, §§ 77 and 80). 121 Likewise**, the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy,** expressly provided for in Article 15(2) of Directive 2002/58, read together with Article 22 of Directive 95/46, where their rights have been infringed (see, by analogy, judgments of 7 May 2009, Rijkeboer, C-553/07, EU:C:2009:293, paragraph 52, and of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 95). 122 With respect to the rules relating to the security and protection of data retained by providers of electronic communications services, it must be noted that Article 15(1) of Directive 2002/58 does not allow Member States to derogate from Article 4(1) and Article 4(1a) of that directive. Those provisions require those providers to take appropriate technical and organisational measures to ensure the effective protection of retained data against risks of misuse and against any unlawful access to that data. **Given the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it, the providers of electronic communications services must, in order to ensure the full integrity and confidentiality of that data, guarantee a particularly high level of protection and security by means of appropriate technical and organisational measures. In particular, the national legislation must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period** (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraphs 66 to 68). 123 **In any event, the Member States must ensure review, by an independent authority, of compliance with the level of protection guaranteed by EU law with respect to the protection of individuals in relation to the processing of personal data, that control being expressly required by Article 8(3) of the Charter** and constituting, in accordance with the Court's settled case-law, an essential element of respect for the protection of individuals in relation to the processing of personal data. If that were not so, persons whose personal data was retained would be deprived of the right, guaranteed in Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim seeking the protection of their data (see, to that effect, the Digital Rights judgment, paragraph 68, and the judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraphs 41 and 58).
4.	OPINION OF ADVOCATE GENERAL MENGOZZI, delivered on 8 September 2016, Opinion 1/15: PNR data, transfer to a non-EU country, use of data for law-enforcement	69. The agreement envisaged is therefore intended to allow Canada to process the PNR data of passengers carried by airlines flying between the European Union and Canada, for the purpose of combating terrorism and other serious transnational crime while safeguarding the right to respect for privacy and the right to protection of personal data under the conditions laid down in the agreement envisaged itself. 170. That data, taken as a whole, touches on the area of the privacy, indeed intimacy, of persons and indisputably relates to one or more

	and security purposes, safeguards	'identified or identifiable individual or individuals'. (58) **There can therefore be no doubt, in the light of the Court's case-law, that the systematic transfer of PNR data to the Canadian public authorities, access to that data and the use of that data and its retention for a period of five years by those public authorities and also, where relevant, its subsequent transfer to other public authorities, including those of third countries, under the terms of the agreement envisaged, are operations which fall within the scope of the fundamental right to respect for private and family life guaranteed by Article 7 of the Charter and to the 'closely connected' (59) but nonetheless distinct right to protection of personal data guaranteed by Article 8(1) of the Charter and constitute an interference with those fundamental rights.** 171. In fact, the Court has already held, with regard to Article 8 of the ECHR, on which Articles 7 and 8 of the Charter are based, (60) that the communication of personal data to third parties, in that particular case a public authority, constitutes an interference within the meaning of that article (61) and that the obligation to retain that data, required by the public authorities, and subsequent access of the competent national authorities to data relating to a person's private life also constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter . (62) Likewise, an EU act prescribing any form of processing of personal data constitutes an interference with the fundamental right, laid down in Article 8 of the Charter, to protection of such data. (63) That assessment applies, mutatis mutandis, with regard to an EU act in the form of an international agreement concluded by the Union, such as the agreement envisaged, which is designed, in particular, to enable one or more public authorities of a third country to process and retain the personal data of air passengers. The lawfulness of such an act depends on its respect for the fundamental rights protected in the EU legal order, (64) especially those guaranteed by Articles 7 and 8 of the Charter. Par. 184 – acknowledges that the transfer of data to the Canadian authorities is not consensual. Par. 190-195: meets the legal basis and general interest of the EU requirements. 205. That point having been clarified, **I do not believe that there are any real obstacles to recognising that the interference constituted by the agreement envisaged is capable of attaining the objective of public security, in particular the objective of combating terrorism and serious transnational crime, pursued by that agreement.** On **strict necessity**: 210. I shall therefore concentrate on the following eight points, which were specifically raised in the request for an opinion or which were discussed between the interested parties during the proceedings before the Court, namely the categories of PNR data covered by the agreement envisaged, the sufficiently precise nature of the purpose for which the processing of PNR data is authorised, the identification of the competent authority responsible for the processing of PNR data, the automated processing of PNR data, access to the PNR data, the retention of the PNR data, the subsequent transfer of the PNR data, and, last, measures of surveillance and judicial review provided for in the agreement envisaged. Par. 328: 2. The agreement envisaged is compatible with Article 16 TFEU and Articles 7 and 8 and Article 52(1) of the Charter of Fundamental Rights of the European Union, **provided that:** – the categories of Passenger Name Record **(PNR) data** of airline

		passengers listed in the annex to the agreement envisaged **are clearly and precisely worded and sensitive data, within the meaning of the agreement envisaged, is excluded from the scope of that agreement**; – **offences** coming within the definition of serious transnational crime, provided for in Article 3(3) of the agreement envisaged, **are listed exhaustively** in the agreement or in an annex thereto; – the agreement envisaged identifies **in a sufficiently clear and precise manner the authority responsible for processing the Passenger Name Record data**, in such a way as to ensure the protection and security of those data; – the agreement envisaged **expressly specifies the principles and rules applicable to both the pre-established scenarios or assessment criteria and the databases with which the Passenger Name Record data is compared in the context of the automated processing of that data**, in such a way that the number of 'targeted' persons can be limited, to a large extent and in a non-discriminatory manner, to those who can be reasonably suspected of participating in a terrorist offence or serious transnational crime; – the agreement envisaged specifies that **only the officials of the Canadian competent authority are to be authorised to access the Passenger Name Record data** and lays down objective criteria that enable the number of those officials to be specified; – the agreement envisaged indicates, stating the reasons, **precisely why it is objectively necessary to retain all Passenger Name Record data for a maximum period of five years**; – where the maximum five-year retention period for the Passenger Name Record data is considered necessary, the agreement envisaged ensures that all the Passenger Name Record data that would enable an airline passenger to be directly identified is **'depersonalised' by masking;** – the agreement envisaged makes the examination carried out by the Canadian competent authority relating to the level of protection afforded by other Canadian public authorities and by those of third countries, and also any decision to disclose Passenger Name Record data, on a case-by-case basis, to those authorities, subject to **ex ante control by an independent authority or a court;** – **the intention to transfer Passenger Name Record data of a national of a Member State of the European Union to another Canadian public authority or to a public authority of a third country is notified in advance to the competent authorities of the Member State in question and/or to the European Commission before any communication takes place;** – the agreement envisaged systematically ensures, by a clear and precise rule, **control by an independent authority**, within the meaning of Article 8(3) of the Charter of Fundamental Rights of the European Union, of respect for the private life and protection of the personal data of passengers whose Passenger Name Record data is processed; and – the agreement envisaged makes clear that **requests for access, rectification and annotation made by passengers not present on Canadian territory may be submitted, either directly or by means of**

		an administrative appeal, to an independent public authority. 3. The agreement envisaged **is incompatible with Articles 7 and 8 and Article 52(1)** of the Charter of Fundamental Rights of the European Union **in so far as:** – Article 3(5) of the agreement envisaged allows, beyond what is strictly necessary, the **possibilities of processing Passenger Name Record data to be extended, independently of the purpose, stated in Article 3 of that agreement, of preventing and detecting terrorist offences and serious transnational crime;** – Article 8 of the agreement envisaged provides for the processing, use and retention by Canada of Passenger Name Record data containing **sensitive data;** – **Article 12(3) of the agreement envisaged confers on Canada, beyond what is strictly necessary, the right to make disclosure of information subject to reasonable legal requirements and limitations;** – Article 16(5) of the agreement envisaged authorises Canada to retain Passenger Name Record data for up to five years for, in particular, any specific action, review, investigation or judicial proceedings, **without a requirement for any connection with the purpose, stated in Article 3 of that agreement, of preventing and detecting terrorist offences and serious transnational crime; and** – Article 19 of the agreement envisaged allows Passenger Name Record data to be transferred to a public authority in a third country **without the Canadian competent authority, subject to control by an independent authority, first being satisfied that the public authority in the third country in question to which the data is transferred cannot itself subsequently communicate the data to another body, where relevant, in another third country.**
5.	C-230/14, *Weltimmo*, 1.10.2015: applicability of EU Member State data protection law, determining the responsible national data protection authority	26 In order to achieve that objective and to ensure that individuals are not deprived of the protection to which they are entitled under that directive, recital 18 in the preamble to that directive states that **any processing of personal data in the European Union must be carried out in accordance with the law of one of the Member States and that processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State.** 28 With regard, in the first place, to the concept of 'establishment', it should be noted that recital 19 in the preamble to Directive 95/46 states **that establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements and that the legal form of such an establishment, whether simply a branch or a subsidiary with a legal personality, is not the determining factor** (judgment in Google Spain and Google, C‑131/12, EU:C:2014:317, paragraph 48). Moreover, that recital states that, **when a single controller is established on the territory of several Member States, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities.** 29 As the Advocate General observed, in essence, in points 28 and 32 to 34 of his Opinion, this results in a flexible definition of the concept of 'establishment', which departs from a formalistic approach whereby

		undertakings are established solely in the place where they are registered. Accordingly, **in order to establish whether a company, the data controller, has an establishment,** within the meaning of Directive 95/46, in a Member State other than the Member State or third country where it is registered, **both the degree of stability of the arrangements and the effective exercise of activities in that other Member State must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned. This is particularly true for undertakings offering services exclusively over the Internet.** 30 In that regard, it must, in particular, be held, in the light of the objective pursued by that directive, consisting in ensuring effective and complete protection of the right to privacy and in avoiding any circumvention of national rules, **that the presence of only one representative can, in some circumstances, suffice to constitute a stable arrangement if that representative acts with a sufficient degree of stability through the presence of the necessary equipment for provision of the specific services concerned in the Member State in question.** 34 In the second place, it is necessary to establish **whether the processing of personal data at issue is carried out 'in the context of the activities' of that establishment.** **37 ... the Court has already had occasion to state that the operation of loading personal data on an Internet page must be considered to be 'processing' within the meaning of Article 2(b) of Directive 95/46** 54 It thus follows from Article 28(6) of Directive 95/46 that **the supervisory authority of a Member State, to which a complaint has been submitted, on the basis of Article 28(4) of that directive, by natural persons in relation to the processing of their personal data, may examine that complaint irrespective of the applicable law,** and, consequently, even if the law applicable to the processing of the data concerned is that of another Member State. 55 However, in that case, the powers of that authority **do not necessarily include all of the powers conferred on it in accordance with the law of its own Member State.**
6.	C-131/12, *Google Spain*, 13.05.2014: activities of search engines, processing of personal data, territorial scope of Directive 95/46/EC	28 Therefore, it must be found that, in **exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results.** As those operations are referred to expressly and unconditionally in Article 2(b) of Directive 95/46, **they must be classified as 'processing'** within the meaning of that provision, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data. 29 Nor is the foregoing finding affected by the fact that those data have already been published on the internet and are not altered by the search engine. 31 Furthermore, it follows from the definition contained in Article 2(b) of Directive 95/46 that, whilst the alteration of personal data indeed constitutes processing within the meaning of the directive, the other operations which are mentioned there do not, on the other hand, in any way require that the personal data be altered.

		33 It is the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity and which **must, consequently, be regarded as the 'controller' in respect of that processing pursuant to Article 2(d).** 60 It follows from the foregoing that the answer to Question 1(a) is that Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that **processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State.** 88 In the light of all the foregoing considerations, the answer to Question 2(c) and (d) is that Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in fact satisfied, the operator of a search engine **is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.** 99 It follows from the foregoing considerations that the answer to Question 3 is that Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, when appraising the conditions for the application of those provisions, it should inter alia be examined whether the data subject has a right that the information in question relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name, without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject. As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, **those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question.**
7.	Case C - 201/14, *Smaranda Bara and Others v Președintele Casei Națională de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF)*, 01.10.2015: tax data, transfer of tax data by one public	28 By its fourth question, the referring court asks, in essence, whether Articles 10, 11 and 13 of Directive 95/46 must be interpreted as precluding national measures, such as those at issue in the main proceedings, which allow **a public administrative body in a Member State to transfer personal data to another public administrative body and their subsequent processing, without the data subjects being informed of that transfer and processing.** 37 It is true that Article 315 of Law No 95/2006 expressly provides that 'the data necessary to certify that the person concerned qualifies as an insured person are to be communicated free of charge to the health insurance funds by the authorities, public institutions or other institutions in accordance with a protocol'. **However, it is clear from the**

	administration to the health insurance authority, restrictions of data subjects' rights, legal basis	**explanations provided by the referring court that the data necessary for determining whether a person qualifies as an insured person, within the meaning of the abovementioned provision, do not include those relating to income,** since the law also recognises persons without a taxable income as qualifying as insured. **38 In those circumstances, Article 315 of Law No 95/2006 cannot constitute, within the meaning of Article 10 of Directive 95/46, prior information enabling the data controller to dispense with his obligation to inform the persons from whom data relating to their income are collected as to the recipients of those data.** Therefore, it cannot be held that the transfer at issue was carried out in compliance with Article 10 of Directive 95/46. 39 It is necessary to examine whether Article 13 of the directive applies to that failure to inform the data subjects. It is apparent from Article 13(1)(e) and (f) that Member States may restrict the scope of the obligations and rights provided for in Article 10 of the same directive when such a restriction constitutes a necessary measure to safeguard 'an important economic or financial interest of a Member State […], including monetary, budgetary and taxation matters' or 'a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e)'. Nevertheless, Article 13 expressly requires that such restrictions are imposed by legislative measures. 40 Apart from the fact, noted by the referring court, that data relating to income are not part of the personal data necessary for the determination of whether a person is insured, it must be observed that Article 315 of Law No 95/2006 merely envisages the principle of the transfer of personal data relating to income held by authorities, public institutions and other institutions. **It is also apparent from the order for reference that the definition of transferable information and the detailed arrangements for transferring that information were laid down not in a legislative measure but in the 2007 Protocol agreed between the ANAF and the CNAS, which was not the subject of an official publication.** 43 It follows that, in accordance with Article 11(1)(b) and (c) of Directive 95/46, in the circumstances of the case in the main proceedings, **the processing by the CNAS of the data transferred by the ANAF required that the subjects of the data be informed of the purposes of that processing and the categories of data concerned.**