EHRC 2016/31
Europees Hof voor de Rechten van de Mens
27 oktober 2015, 62498/11.
(Raimondi (President)
Hirvelä
Nicolaou
Tsotsoria
Mahoney
Wojtyczek
Vehabovic)

R.E.
tegen
Verenigd Koninkrijk

Inmenging privé-communicatie, Covert surveillance, Waarborgen verschoningsgerechtigden, Vertrouwelijke consultatie advocaat en cliënt, Voorzienbaarheid, Noodzakelijkheid

[EVRM - 8]

» Samenvatting

Klager is minderjarig en wordt verdacht van betrokkenheid bij een moord op een politieman door dissidente Republikeinen in Noord-Ierland. Hij is tot driemaal toe gearresteerd om met de politie te spreken. Bij de derde keer vraagt zijn advocaat om te verzekeren dat de gesprekken tussen hem en de klager niet aan ‘covert surveillance’ zullen worden onderworpen, maar dit kon bevestigd noch ontkend worden. Volgens klager is het regime voor ‘covert surveillance’ in strijd met art. 8 EVRM. De eerste vraag die het Hof daarbij heeft te beantwoorden is of in dit geval de heel strenge eisen moeten worden gesteld die het gebruikelijk stelt bij interceptie van telefoongesprekken, of de iets lichtere die het normaliter stelt bij ‘gewone’ gevallen van surveillance. Het Hof geeft toe dat het in eerdere rechtspraak de strenge eisen inderdaad alleen bij telefoontaps heeft gesteld, maar stelt voorop dat het heeft aangenomen, bijvoorbeeld in Bykov, dat deze eisen ook moeten worden gesteld als een andere vorm van surveillance ‘virtually identical’ is aan telefoontappen (Bykov t. Rusland, EHRM 10 maart 2009 (GK), nr. 4378/02 «EHRC» 2009/69 m.nt. Ölçer). De doorslaggevende factor voor de toepasselijke test is de mate van inbreuk op het individuele recht op bescherming van het privéleven. In dit geval ging het om surveillance van juridische consultaties tussen advocaat en cliënt, waarbij geldt dat een bijzondere mate van bescherming nodig is in verband met de vertrouwelijkheid van deze relatie. Het surveilleren van deze consultatie vormt een ‘extremely high degree of intrusion’ in de art. 8-rechten, die nog verder gaat dan die in Bykov. Gelet daarop moeten dezelfde strenge eisen worden gesteld als in het geval van telefoontaps. Het Hof onderwerpt dan het bestaande ‘RIPA II’-regime aan deze toets, waarbij het de regels aanvaardbaar acht waar het gaat om de duur, de selectie van de relevante persoon en de maatregelen rondom voortzetting en beëindiging, maar waarbij het kritisch is waar het gaat om het onderzoeken, bewaren en gebruiken van de verkregen gegevens, en waar het gaat om het delen van deze gegevens met derde partijen. Deze kritiek is zodanig dat het Hof vaststelt dat art. 8 EVRM niet voldoende is gerespecteerd. De tweede vraag die het Hof is voorgelegd is of het redelijk was om de gesprekken te monitoren tussen klager als ‘vulnerable person’ en een ‘appropriate adult’. Het Hof neemt aan dat hierop het lichtere regime van toepassing is en concludeert dat in dit licht wel voldoende waarborgen zijn geboden en er geen schending is van art. 8 EVRM in dit opzicht.

beslissing/besluit

» Uitspraak

I. Alleged violation of Article 8 of the Convention

97. The applicant complained that the regime for covert surveillance of consultations between detainees and their lawyers, medical personnel, and appropriate adults was in breach of Article 8 of the Convention, which reads as follows:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

98. The Government contested that argument.

99. Following receipt of the Government's observations, the applicant accepted that he did not consult with any medical personnel until 7 May 2010, by which time the High Court had directed that consultations with his solicitor and his medical advisor should not be subject to covert surveillance (see paragraphs 20 – 21 above). He therefore accepted that he could not have suffered any interference with his Article 8 rights in this regard.

A. Lawyer/client consultations

1. Admissibility

100. The Court is satisfied that this complaint raises complex issues of fact and law, such that it cannot be rejected as manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention. It further considers that the complaint is not inadmissible on any other grounds. It must therefore be declared admissible.

2. Merits

a. The parties' submissions

. The applicant

101. The applicant argued that Article 8 was clearly engaged by the covert surveillance of consultations with his legal advisor. Although he accepted that the purposes identified in the legislation permitting covert surveillance amounted to a legitimate aim, he maintained that the relevant legal framework failed both the "quality of law" and "necessity" tests under paragraph 2 of Article 8 of the Convention.

102. The applicant submitted that the combined effect of Part II of RIPA, the Revised Code and the PSNI Service Procedure did not provide, in relation to covert surveillance of lawyer/client consultations, the "adequate and effective guarantees against abuse" required by Article 8 of the Convention, especially when compared with the clear and precise statutory guidelines outlined in Part I of RIPA in respect of the interception of communications (see *Kennedy v. the United Kingdom*, no. 26839/05, 18 May 2010).

103. Unlike Part I of RIPA, Part II, read together with the Revised Code, did not indicate with sufficient clarity the test for authorising covert surveillance of lawyer-client consultations; in particular, paragraph 4.12 of the Revised Code only provided examples of when surveillance intended to result in the acquisition of legally privileged material would be permitted, for example "where there is a threat to life or limb, or to national security". In any case, the applicant argued that in view of the importance and sensitivity of the issue, any "threat to life or

limb" should have to be "real or immediate".

104. Moreover, the procedures for the handling, dissemination and destruction of legally privileged material were not sufficiently precise and did not satisfy the minimum safeguards identified by the Court in *Valenzuela Contreras v. Spain*, 30 July 1998, *Reports of Judgments and Decisions* 1998 V. Although the applicant acknowledged that *Valenzuela Contreras* was an "interception case", he argued that the principles derived from the Court's "interception" case-law could be "read across" to the present case because, first, the Court had not drawn a distinction between the principles which applied in interception cases and covert-surveillance cases; secondly, it was the nature and degree of intrusion in certain types of covert surveillance cases which allowed the Court to "read across" from the principles set out in interception cases; thirdly, any distinction was therefore not appropriate when dealing with covert surveillance of the kind in issue in the present case; and finally, given that both types of case involved the handling of material obtained as a result of listening to and recording private conversations, it was difficult to see what valid distinction could be made between an interception operation and a covert-surveillance operation of the kind at issue in the present case.

105. The applicant pointed to paragraph 9.3 of the Revised Code, which provided that each public authority had to ensure that arrangements were in place for the secure handling and destruction of material obtained through directed or intrusive surveillance. This was the function of the PSNI Service Procedure, which went much further than the Code in providing for limits on dissemination, storage, access, retention and destruction. However, it was not in force at the relevant time and, in any case, the applicant contended that such important matters should not be left to the discretion of the individual public authorities.

106. The applicant acknowledged the existence of the July 2005 Criminal Procedure and Investigations Act 1996 Code of Practice for Northern Ireland ("the CIPA Code"), which set out the manner in which police officers were to record, retain and reveal to the prosecutor material obtained in a criminal investigation which may be relevant to the investigation. However, he submitted that the different legislative schemes taken together did not present a clear picture or provide sufficient clarity to enable an individual to be able to ascertain the arrangements for handling any material obtained as a result of covert surveillance of his legal consultations.

107. Finally, the applicant argued that even if the interference with his Article 8 rights was "in accordance with the law", it was not "necessary in a democratic society". Consultations between a detainee and his legal advisor were particularly sensitive in view of the fundamental rights at stake, and yet the detainee could only avoid covert surveillance by electing not to speak to his lawyer. As such, the legislation had the potential to undermine some of the basic protections underlying the criminal justice system in the United Kingdom.

b. The Government

108. The Government accepted that the applicant could claim to be a victim of an alleged violation of Article 8 in relation to his legal consultations with his solicitor between 4 May 2010 and 6 May 2010. It also noted that it did not appear to be in dispute that the surveillance pursued a legitimate aim for the purposes of Article 8 § 2 of the Convention.

109. The Government argued that any interference was "in accordance with the law": it had its basis in domestic law; the law in question was accessible as it took

the form of primary and secondary legislation and a published Revised Code (the Government accepted that it could not rely on the PSNI Service Procedure in the present case as it was not issued until 22 June 2010); and finally, the law was sufficiently foreseeable.

110. In particular, the law at issue indicated the scope of the PSNI's discretionary power with sufficient clarity, as it afforded citizens an adequate indication of the circumstances in which the PSNI was empowered to authorise intrusive surveillance of legal consultations in police stations. Insofar as the applicant argued that the Revised Code did not satisfy the detailed requirements set out in *Valenzuela-Contreras v. Spain* (because it did not make provision for the destruction of legally privileged material obtained as a result of intrusive surveillance and did not set a test for the circumstances in which retention or onward dissemination could occur), the Government contended that that case concerned interception powers and had not been applied by the Court in cases concerning covert surveillance. Indeed, the Government maintained that in view of the wide range of surveillance powers, and the wide range of circumstances in which they might properly be deployed, it would be inappropriate as a matter of principle to be overly prescriptive as to the specific features that must be present within any surveillance regime.

111. In the Government's submission, the true test was therefore whether the "manner of [the] exercise" of the PSNI's discretionary power to conduct surveillance of legal consultations was indicated in the law with sufficient clarity to give the individual adequate protection against arbitrary interference; and that test was clearly satisfied in the present case. The Revised Code obliged the PSNI to put in place arrangements for the secure handling, storage and destruction of material obtained through the use of directed or intrusive surveillance; if the PSNI obtained legally privileged material through intrusive surveillance of legal consultations, that material had to be kept separate from any criminal investigation or prosecution and handled in accordance with the Revised Code; pursuant to the fifth data protection principle in the Data Protection Act 1998, the retained material would in general need to be destroyed once its retention was no longer necessary for the purpose for which the PSNI had been processing it; if legally privileged material was disseminated by the PSNI to another body, it had to be accompanied by a clear warning that it was subject to legal privilege, the Surveillance Commissioners would have to be notified during their next inspection and any dissemination would have to be compatible with the Data Protection Act; and finally, insofar as intrusive surveillance by the PSNI resulted in the acquisition of material that was not legally privileged, its retention and potential use or disclosure in any subsequent criminal proceedings was governed by the detailed Criminal Procedure and Investigations Act 1996 Code of Practice.

112. The Government referred to *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, §§ 92 – 92, 28 June 2007, which indicated that the Court should consider evidence of the actual operation of the system of surveillance, in particular whether it was working properly or whether it was subject to abuse. In the United Kingdom only one intrusive surveillance order had been granted in the three years since the 2010 Order came into force. It was therefore clear that in practice authorisations were only being granted in highly exceptional cases.

113. In the alternative, the Government argued that if the standards developed in the context of interception of communications ought to be applied in the

present case, the above regime satisfied them.

114. The Government further submitted that the regime satisfied the requirement of "necessity". Indeed, the Contracting States enjoyed a wide margin of appreciation in determining the precise conditions under which a system of covert surveillance was to be operated; and in the present case the safeguards offered adequate and effective guarantees against abuse: only the Chief Constable or Deputy Chief Constable could in general grant an authorisation for intrusive surveillance of legal consultations; save in cases of urgency, such authorisation would not take effect unless and until it was approved by a Surveillance Commissioner; even in urgent cases the ordinary Surveillance Commissioners retained the power to quash any order retrospectively and order the destruction of any relevant records; the regime was overseen by the Chief Surveillance Officer, who was independent of the PSNI and had to have held high judicial office; the regime was subject to further judicial oversight in the form of the Investigatory Powers Tribunal, which had jurisdiction to hear complaints by any person regarding the operation of the regime and had power to order appropriate relief; and finally, the Revised Code required that knowledge of matters subject to legal privilege be kept separate from law enforcement investigations or criminal prosecutions.

b. The Court's assessment

. The existence of an interference

115. Insofar as the applicant's complaints concern the regime for conducting covert surveillance of consultations between detainees and their legal advisors, the Government have accepted that he can claim to be a victim of the alleged violation.

116. In this regard, it is now well-established that an individual may under certain conditions claim to be the victim of a violation occasioned by the mere existence of legislation permitting secret measures without having to demonstrate that such measures were in fact applied to him (*Klass and Others v. Germany*, 6 September 1978, § 34, Series A no. 28).

117. Consequently, the Court will proceed on the basis that there has been an "interference", within the meaning of Article 8 § 2 of the Convention, with the applicant's right to respect for his private life.

b. Was the interference justified?

118. In order to be justified under Article 8 § 2 of the Convention, the interference must be "in accordance with the law", in pursuit of a legitimate aim, and "necessary in a democratic society".

119. In respect of Part I of RIPA the Court considered that the interception regime pursued the legitimate aims of the protection of national security and the prevention of disorder and crime (*Kennedy v. the United Kingdom*, no. 26839/05, § 155, 18 May 2010). The Court considers that the surveillance regime under Part II of RIPA pursues the same legitimate aims and this has not been disputed by the parties. It therefore falls to the Court to consider the remaining two questions: was the regime "in accordance with the law", and was it "necessary" to achieve the legitimate aim pursued?

120. The requirement that any interference must be "in accordance with the law" under Article 8 § 2 will only be met when three conditions are satisfied: the impugned measure must have some basis in domestic law; the domestic law must be compatible with the rule of law and accessible to the person concerned; and the person concerned must be able to foresee the

consequences of the domestic law for him (see, among many other authorities, *Rotaru v. Romania* [GC], no. 28341/95, § 52, ECHR 2000 V, *Liberty and Others v. the United Kingdom*, no. 58243/00, § 59, 1 July 2008, and *Iordachi and Others v. Moldova*, no. 25198/02, § 37, 10 February 2009).

121. In the present case it is not in dispute that the surveillance regime had a basis in domestic law, namely RIPA and the Revised Code of Practice. Moreover, both RIPA and the Revised Code were public documents – like the Interception of Communications Code of Practice, the Revised Code is available on the internet. This being so, the Court accepts that the relevant domestic law was adequately accessible for the purposes of Article 8 of the Convention.

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).

123. In *Valenzuela Contreras v. Spain*, cited above, § 59, an interception-of-communications case, the Court set the standard high, finding that the relevant legislation was not adequately foreseeable because neither the Constitution nor the Code of Criminal Procedure included

"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."

124. Similarly, in considering whether an interception of communications was "necessary in a democratic society, in *Weber and Saravia v. Germany*, cited above, § 95 the Court stated:

"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, 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)."

125. Consequently, in *Kennedy v. the United Kingdom*, cited above, § 155 the Court examined in some detail the provisions of both RIPA and the Interception of Communications Code of Practice insofar as they concerned the definition of the categories of people liable to have their telephones tapped by judicial order; the nature of the offences which might give rise to such an order; a limit on

the duration of telephone tapping; the provisions on duration, renewal and cancellation of intercept warrants; the procedure for examining, using and storing the data; the general safeguards which applied to the processing and communication of intercept material; the destruction of intercept material; the keeping of records of intercept warrants; and the supervision of the RIPA regime.

126. However, the Government have argued that in its case-law the Court has distinguished between the minimum safeguards required in interception-of-communication cases and those required in other surveillance cases. As the present case concerns covert surveillance and not the interception of communications, so the Government submitted, the relevant test should be less strict; namely, whether the manner of the exercise of the authorities' discretionary power to conduct surveillance of legal consultations was indicated in the law with sufficient clarity to give the individual adequate protection against arbitrary interference.

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.

128. In *Bykov v. Russia* [GC], no. 4378/02, § 78, 10 March 2009, a case which concerned the recording of a private conversation by way of a radio transmitting device, the Court made it clear that the degree of precision required of the law would depend upon the particular subject-matter of the case. It held that in terms of the nature and degree of the intrusion involved the recording of the conversation in that case was "virtually identical" to telephone tapping and, this being so, it should assess the relevant legislation using the same principles as applied to the interception of communications. Nevertheless, although it cited *Valenzuela-Contreras*, it defined the relevant test as being whether the law was sufficiently clear to give citizens an adequate indication of the circumstances in which and the conditions on which public authorities were empowered to resort to a secret interference with the right to respect for private life and correspondence. It did not refer to the stricter requirements set out in that judgment, although it is arguable that it was not necessary on the facts of that case as the legal discretion of the authorities to order the interception had not been subject to any conditions and the scope and manner of its exercise had not been defined.

129. In *Uzun v. Germany*, no. 35623/05, § 66, ECHR 2010 (extracts) the Court accepted that the monitoring of a car's movements by GPS interfered with the applicant's Article 8 rights. However, it distinguished this kind of surveillance from other methods of visual or acoustic surveillance which were generally more susceptible of interfering with Article 8 rights because they disclosed more information on a person's conduct, opinions or feelings. Therefore, the Court indicated that, while it would not be barred from drawing inspiration from the principles set up and applied in the specific context of surveillance of telecommunications, those principles would not be directly applicable in a case concerning surveillance of movements in public places via GPS because such a measure "must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations". Instead, the Court applied the more general principles on adequate protection against arbitrary interference with Article 8 rights (see, for example, *Weber and Saravia*, cited above,

§ 94, and the test applied in *Bykov*, set out at paragraph 128 above).

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).

135. In *Kennedy*, the Court noted that the warrant authorising interception specified the person or premises in respect of which it had been ordered. Although intrusive surveillance is not usually authorised by virtue of a warrant, pursuant to paragraph 6.19 of the Revised Code the application for authorisation must set out the nature of the surveillance; the residential premises or private vehicle in relation to which the surveillance will take place, where known; the identities, where known, of those to be the subject of the surveillance; an explanation of the information which it is desired to obtain as a result of the surveillance; details of any potential collateral intrusion and why that intrusion is justified; details of any confidential information likely to be obtained as a consequence of the surveillance; the reasons why the surveillance is considered proportionate to what it seeks to achieve; and a record of whether authorisation was given and refused, by whom, and the time and date when this happened (see paragraph 48 above). The senior authorising officer may only grant authorisation if he considers it necessary and proportionate, and, unless it is an urgent case, this decision is subject to further scrutiny by a Surveillance Commissioner before the authorisation takes effect (see paragraph 56 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.

142. Consequently, the Court considers that, to this extent, during the relevant period of the applicant's detention (4 – 6 May 2010 – see paragraphs 18 – 20 above), the impugned surveillance measures, insofar as they may have been applied to him, did not meet the requirements of Article 8 § 2 of the Convention as elucidated in the Court's case-law.

143. There has therefore been a breach of Article 8 of the Convention.

B. Consultations between a detainee who is a "vulnerable person" and an appropriate adult

1. Admissibility

144. The Court is satisfied that this complaint raises complex issues of fact and law, such that it cannot be rejected as manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention. It further considers that the complaint is not inadmissible on any other grounds. It must therefore be declared admissible.

2. Merits

a. The parties' submissions

. The applicant

145. The applicant contended that the regime covering covert surveillance between a detainee who was a "vulnerable person" within the meaning of the Code of Practice and an "appropriate adult" (see paragraph 13 above) was not "in accordance with the law" as required by paragraph 2 of Article 8 of the Convention. In particular, he submitted that even though

these consultations were not protected by legal professional privilege, in view of the vulnerability of the detainee they should be as frank as possible. As such, they were analogous to consultations with legal and medical advisors and their covert surveillance should also have been treated as intrusive – rather than directed – surveillance.

146. On account of being treated as directed surveillance, the present regime allowed for surveillance where it was necessary for one of six purposes set out in section 28(3) of RIPA, including for the purpose of assessing any tax, duty, or levy, and the authorisation was proportionate to what was sought to be achieved; the authorisation could be made by a large number of public authorities; the authorisation did not have to be made by officers at a very senior level within those authorities (a Superintendent within the PSNI); and there was no requirement for prior or subsequent supervision or scrutiny of the individual authorisation by a Surveillance Commissioner or any other independent person or body.

147. The applicant further argued that section 28(6) identified a broad range of circumstances in which covert surveillance of consultations with an appropriate adult could take place, and those circumstances were ill-defined in the legislation; the statutory scheme entitled an extensive number of public authorities to engage in such surveillance and therefore reduced the level of foreseeability in terms of an individual being able to regulate their conduct; the number of individuals within those public authorities who could authorise the use of directed surveillance was not narrowly circumscribed; there were no meaningful limitations on the circumstances in which such material could be deployed; and there was a significant absence of any limits in relation to the retention, storage, transmission, dissemination and destruction of such material.

148. The applicant also submitted that the aims identified under section 28(3) of RIPA were not "legitimate"; this was particularly the case in respect of the aim of furthering the collection of taxes, levies and other duties.

149. Finally, and in any case, the applicant contended that the regime in respect of the covert surveillance of the detainee's consultation with an appropriate adult did not satisfy the test of "necessity" in Article 8 § 2 of the Convention. In particular, there was no reason why the authorisation of such surveillance could not be carried out by an independent person with a judicial background.

The Government

150. The Government accepted that the applicant could claim to be a victim of an alleged violation of Article 8 of the Convention in relation to his consultations with his appropriate adult from 4 May 2010 to 8 May 2010 (consultations with the appropriate adult were not affected by the court's direction on 6 May 2010 that the applicant's consultations with his solicitor and medical advisor should not be subject to surveillance).

151. The Government argued that the surveillance of consultations between a detainee and an appropriate adult pursued a legitimate aim. The applicant had only sought an assurance from the PSNI that his consultations would not be subject to covert surveillance. He could therefore only complain about potential surveillance by the PSNI and that body was not permitted to conduct such surveillance to further the collection of taxes, levies or other duties.

152. Furthermore, the Government submitted that the interference with the

applicant's Article 8 rights was similarly justified. There was no close analogy between the meetings with an appropriate adult and consultations with doctors or solicitors, the latter two being subject to legal privilege. This was the reason why consultations with doctors and solicitors were brought within the intrusive surveillance regime and made subject to a test of exceptionality. Appropriate adults, however, were not lawyers and their function was not to provide legal advice or to assist in the preparation of a criminal defence.

153. In any case, the Government argued that the directed surveillance regime contained adequate safeguards against abuse: the PSNI's use of directed surveillance powers was subject to oversight by the Chief Surveillance Commissioner; any individual could complain to the IPT if he was concerned that he might have been subject to directed surveillance and the IPT had the power to grant appropriate relief if any such complaint was found to have substance; and, if criminal proceedings followed, under the court's abuse of process jurisdiction any relevant use of directed surveillance would be subject to further control by the trial judge, both in relation to admissibility of material obtained thereby and in the event of any allegation of abuse or unlawfulness.

b. The Court's assessment

. The existence of an interference

154. Insofar as the applicant complains about the regime for conducting covert surveillance of consultations between detainees and their appropriate adults, the Government have accepted that he can claim to be a victim of the alleged violation.

155. For the reasons set out in paragraphs 115 – 117 above, the Court would agree that there has been an "interference", within the meaning of Article 8 § 2 of the Convention, with the applicant's right to respect for his private life.

b. Was the interference justified?

156. The Court has already noted that in order to be justified under Article 8 § 2 of the Convention the interference must be "in accordance with the law", in pursuit of a legitimate aim, and "necessary" in a democratic society.

157. As with the regime for surveillance of lawyer/client consultations, the Court considers that the regime in question pursues the legitimate aims of protection of national security and the prevention of disorder and crime (see paragraph 119 above). Furthermore, for the reasons set out at paragraph 121 above, the Court finds that the regime had a basis in domestic law, namely Part II of RIPA and the Revised Code of Practice, and that that law was sufficiently accessible. It therefore falls to the Court to decide if the law was adequately foreseeable and whether the interference was "necessary in a democratic society". As the lawfulness of the interference is closely related to the question of its "necessity", the Court will jointly address the foreseeability and the "necessity" requirements (see also *Kennedy*, cited above, § 155).

158. The Court has indicated at paragraph 130 above that the subject-matter of the surveillance and the degree of intrusion will determine the degree of precision with which the law must indicate the circumstances in which and the conditions on which the public authorities are entitled to resort to covert measures. The surveillance of consultations between a vulnerable detainee and an appropriate adult, appointed to assist him or her following an arrest, undoubtedly constitutes a significant degree of intrusion. As such, the present case is distinguishable

from that of *Uzun*, cited above, which concerned the monitoring of a car's movements by GPS and, as a consequence, the collection and storage of data determining the applicant's whereabouts and movements in the public sphere.

159. That being said, the surveillance was not taking place in a private place, such as a private residence or vehicle. Rather, it was being conducted in a police station. Moreover, unlike legal consultations, consultations with an appropriate adult are not subject to legal privilege and do not attract the "strengthened protection" accorded to consultations with lawyers or medical personnel. The detainee would not, therefore, have the same expectation of privacy that he or she would have during a legal consultation. Consequently, the Court does not consider it appropriate to apply the strict standard set down in *Valenzuela-Contreras* and will instead focus on the more general question of whether the legislation adequately protected detainees against arbitrary interference with their Article 8 rights, and whether it was sufficiently clear in its terms to give individuals adequate indication as to the circumstances in which and the conditions on which public authorities were entitled to resort to such covert measures (*Bykov*, cited above, § 76).

160. As it is classified as directed rather than intrusive surveillance, the surveillance of consultations with appropriate adults is permissible in a wider range of circumstances than the surveillance of legal consultations (see paragraph 44 above). In Part II of RIPA, section 28 provides that directed surveillance can take place where the authorising officer (in this case a PSNI officer of the rank of Superintendant or above) believes it is necessary in the interests of national security, for the purposes of preventing or detecting serious crime, in the interests of the economic well-being of the United Kingdom, in the interests of public safety, for the purposes of protecting public health, for the purposes of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department, and for any other purpose specified for the purposes of this subsection by an order of the Secretary of State. Nevertheless, the differences are not so great as they might first appear. The PSNI could not authorise the surveillance of a consultation with an appropriate adult for the purposes of assessing or collecting any tax or levy, and the Secretary of State has not specified any other purpose by way of an order. Consequently, consultations with an appropriate adult can only be subject to surveillance on two additional grounds: the interests of public safety, and protecting public health. Like "national security", both terms are frequently employed in national and international legislation and constitute two of the legitimate aims to which Article 8 § 2 refers. 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.

161. As with intrusive surveillance, RIPA does not provide any limitation on the persons who may be subjected to directed surveillance. However, paragraph 5.8 of the Revised Code, which sets out the information to be included in an application for directed surveillance, is drafted in identical terms to paragraph 6.19, which concerns intrusive surveillance (see paragraph 41 above), and, similarly, the authorising officer may only authorise directed surveillance if he considers it necessary and proportionate. It is true that fewer safeguards exist than in respect of the surveillance of legal consultations. First, the surveillance is not subject to the enhanced authorisation regime which applies to surveillance intended to result in the obtaining of information subject to legal privilege. Secondly, surveillance carried out by the PSNI may be authorised by a police officer at the level of

Superintendent or above, whereas intrusive surveillance may only be authorised by a senior authorising officer, namely the Chief Constable of the PSNI or the Secretary of State. Thirdly, authorisation does not have to be approved by a Surveillance Commissioner. However, while the Court believes these safeguards to be important in the context of intrusive surveillance, particularly that of legal consultations, in the context of surveillance of consultations with appropriate adults the Court considers that no further clarification of the categories of persons liable to be subject to secret surveillance can reasonably be required.

162. With regard to additional safeguards, the Court notes that authorisations for directed surveillance must be regularly reviewed to assess the need for the surveillance to continue (see paragraph 62 above). During a review, the authorising officer who granted or last renewed the authorisation may amend specific aspects of it. He must cancel the authorisation if satisfied that it no longer meets the criteria on which it was authorised. As soon as the decision is taken that it be discontinued, the instruction must be given to stop all surveillance of the subject and the date of the cancellation should be directly recorded.

163. In any case, the written authorisation will cease to have effect (unless renewed or cancelled) at the end of a period of three months beginning with the time it took effect (see paragraph 63 above). Written renewals may only be granted for three months at a time, and in order to grant them the authorising officer must be satisfied that it is necessary for the authorisation to continue for the purposes for which it was given (see paragraph 64 above). All applications for renewal should record whether it is the first renewal or every occasion a renewal was previously authorised; any significant changes to the information in the initial application; the reasons why the authoristion should continue; the content and value to the investigation or operation of the information so far obtained; and the results of regular reviews of the investigation or operation (see paragraph 65 above).

164. Detailed records pertaining to all authorisations must be centrally retrievable within each public authority and be retained for at least three years from the end of each authorisation (see paragraph 73 above). Moreover, it is the role of the surveillance commissioners to keep under review the exercise and performance of the powers and duties conferred by Part II of the Act. In doing so, they have the power to quash authorisations and order the destruction of any records relating to information obtained by authorised conduct (see paragraph 78 above).

165. Other than that which is subject to legal professional privilege, information obtained by secret surveillance may be used in evidence in criminal proceedings. However, the admissibility of such evidence would be subject to the control of the trial judge. In certain circumstances it would also be open to the trial judge to stay a prosecution for abuse of process (see paragraph 153 above).

166. Finally, any citizen who believes that they have wrongfully been subject to surveillance may bring a claim to the IPT and, save for vexatious or frivolous claims, the latter tribunal must determine any such claim. The IPT has the power to award compensation and make such orders as it thinks fit, including the quashing or cancelling of any order and the destruction of any records (see paragraph 79 above).

167. The foregoing considerations are sufficient to enable the Court to conclude that the provisions concerning directed surveillance, insofar as they related to the possible surveillance of consultations between detainees and appropriate adults,

were accompanied by adequate safeguards against abuse.

168. Accordingly, no violation of Article 8 of the Convention can be found under that head.

II. Alleged violation of Article 6 of the Convention

169. The applicant complained of a violation of 6 of the Convention, which provides as relevant:

"1. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law....

... ...

3. Everyone charged with a criminal offence has the following minimum rights:

... ...

(c) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require."

170. In particular, he complained that his ability to communicate effectively with a solicitor in private was damaged in breach of Article 6 § 3(c) of the Convention and that his ability to communicate with an appropriate adult was compromised in breach of Article 6 generally.

171. Although the applicant was charged with the offence of withholding information, he did not stand trial for this or any other offence. Consequently, he cannot complain that any "restriction" imposed on him by virtue of the possibility of covert surveillance deprived him of a fair hearing in breach of Article 6.

172. Furthermore, even if the possibility of covert surveillance of his legal consultations could give rise to an issue under Article 6 § 3(c) of the Convention, the Court recalls that on 6 June 2010 the Administrative Court ordered that there should be no surveillance of the applicant's consultations with his lawyer or doctor pending the outcome of the judicial review proceedings. Consequently, the applicant would have had ample opportunity to consult with both his legal and medical advisors safe in the knowledge that those consultations would not be subject to covert surveillance.

173. In light of the above, the Court considers that the applicant's complaints under Article 6 of the Convention are manifestly ill-founded within the meaning of Article 35 § 3(a) of the Convention.

III. Application of Article 41 of the Convention

174. Article 41 of the Convention provides:

"If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

A. Damage

175. The applicant made no claim for pecuniary damage. However, he claimed six thousand euros (EUR 6,000) in respect of non-pecuniary damage. In particular, he argued that as a vulnerable person with a history of drug and alcohol abuse, anxiety and depression the concern that his legal consultations might be subject to covert surveillance caused him significant distress.

176. The Government argued that a declaration of a breach would be sufficient

just satisfaction. In particular, they argued that there was no evidence that the applicant had experienced any suffering or distress related to the possibility that his legal consultations might have been subject to covert surveillance.

177. The Court agrees that the applicant has submitted no evidence to substantiate his claim that the possibility that his legal consultations were subject to covert surveillance caused him any real suffering or distress. Nevertheless, the applicant was undoubtedly a vulnerable young man at the time of his arrest and the Court is therefore prepared to accept that the possibility of not being able to speak freely with his solicitor was capable of having caused him some anguish. However, the possibility of covert surveillance only existed from 4 May 2010 to 6 May 2010, on which date the Administrative Court ordered that his legal consultations should not be subject to surveillance.

178. The Court therefore awards the applicant EUR 1,500 in respect of non-pecuniary damage.

B. Costs and expenses

179. The applicant also claimed GBP 26,126.08 for the costs and expenses incurred before the Court.

180. The Government argued that that sum was excessive.

181. According to the Court's case-law, an applicant is entitled to the reimbursement of costs and expenses only insofar as it has been shown that these have been actually and necessarily incurred and are reasonable as to quantum. In the present case, regard being had to the documents in its possession and the above criteria, the Court considers it reasonable to award the sum of EUR 15,000 covering costs under all for the proceedings before the Court.

C. Default interest

182. The Court considers it appropriate that the default interest rate should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

For these reasons, the Court, unanimously,

1. *Declares* the complaints under Article 8 of the Convention admissible and the remainder of the application inadmissible;

2. *Holds* that insofar as the applicant complains about the covert surveillance of legal consultations, there has been a violation of Article 8 of the Convention;

3. *Holds* that insofar as the applicant complains about the covert surveillance of consultations between detainees and their appropriate adults, there has been no violation of Article 8 of the Convention;

4. *Holds*

(a) that the respondent State is to pay the applicant, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, the following amounts, to be converted into the currency of the respondent State at the rate applicable at the date of settlement:

(i) EUR 1,500 (one thousand five hundred euros), plus any tax that may be chargeable, in respect of non-pecuniary damage;

(ii) EUR 15,000 (fifteen thousand euros), plus any tax that may be chargeable to the applicant, in respect of costs and expenses;

(b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amounts at a rate equal to the

marginal lending rate of the European Central Bank during the default period plus three percentage points;

5. *Dismisses* the remainder of the applicant's claim for just satisfaction.

» Noot

1. In *R.E.* t. *Verenigd Koninkrijk* onderschrijft het EHRM unaniem de sterke waarborgen ten aanzien van de inmenging in een gedetineerde zijn communicatie met verschoningsgerechtigden. De rechters gaan in op de vraag of de Britse juridische waarborgen voor *covert surveillance* met betrekking tot vertrouwelijke gesprekken met derden, waaronder advocaten en een 'aangewezen' volwassene (een soort van vertrouwenspersoon voor kwetsbare gedetineerden), in strijd is met art. 8 EVRM. Veruit de belangrijkste vraag die het Hof daarbij beantwoordt is of in het geval van de vertrouwelijke advocaat-cliënt-consultatie de veel strengere waarborgen voor *intrusive surveillance* gelden, zoals, voor bijvoorbeeld, het aftappen van telefoongesprekken in iemands huis, of de iets lichtere waarborgen die normaliter gesteld worden bij 'gewone' gevallen van *covert surveillance*. Hieronder vallen onder andere het opslaan van metadata van locatiegegevens van voertuigen. Het EHRM oordeelt uiteindelijk dat de privacywaarborgen voor de surveillance van vertrouwelijke gesprekken tussen advocaten en (gedetineerde) cliënten zeer sterk zijn en dat dit getoetst dient te worden, niet aan de hand van het het type surveillance, maar op basis van de omstandigheden en de mate van inmenging in iemands privéleven. Deze annotatie focust op de heimelijke surveillance van de vertrouwelijke advocaat-cliënt-gesprekken en niet op de communicatie met de 'aangewezen' volwassene. De reden hiervoor is dat het politieke en publieke debat rondom heimelijke obervatie en monitoring van advocaten actueel is en dat het EHRM in het geval van de vertouwenspersoon geen schending van art. 8 EVRM zag. In het bijzonder richt deze noot zich op de voorzienbaarheid van de surveillance van vertrouwelijke advocaat-cliënt-gesprekken en de noodzakelijk van die inmenging in een democratische samenleving.

Surveillance van vertrouwelijke advocaat-cliënt-gesprekken

2. De gesprekken tussen de minderjarige gedetineerde klager en zijn advocaat bleken tussen 4 en 6 mei 2010 heimelijk te zijn geobserveerd. De Britse wet- en regelgeving – Deel II van de *Regulations of Investigatory Powers Act 2000* (RIPA) en de *Covert Surveillance Code of Practices* – stond dit toentertijd onder bepaalde omstandigheden toe (sindsdien is er nieuwe regelgeving met betrekking tot *covert surveillance* van de vertrouwelijk advocaat-cliënt-gesprekken tijdens detentie ingevoerd: waaronder de *Regulation of Investigatory Powers (Extension of the Autorisation Provisions: Legal Consulations) Order* 2010, de '2010 Order', en op 22 juni 2010, de *Police Service of Northern Ireland Police Service Procedure*, "*Covert Surveillance of Legal Consultations and the Handling of Legally Priviledged Material*"). Maar omdat dat toen nog niet van kracht was, oordeelde het EHRM in dit arrest dat ondanks de aanpassing aan wet- en regelgeving er een inbreuk was gemaakt op het privéleven van de klager. Deze inmenging diende echter wel een legitiem doel: namelijk het beschermen van de nationale veiligheid of opsporen van ernstige misdrijven (par. 140). Ook kende de inmenging een wettelijke basis namelijk RIPA en de *Covert Surveillance Code of Practices*. Dus aangezien er een wettelijke basis was voor de inmenging op het recht op privacy en de inmenging een legitiem doel diende, toetste het EHRM in dit arrest de voorzienbaarheid van het heimelijk monitoren van de communicatie tussen een raadsman en zijn

gedetineerde cliënt in combinatie met de noodzaak van inmenging in een democratische samenleving. De uitspraak is grotendeels gebaseerd op EHRM-jurisprudentie: namelijk de *Kennedy*-uitspraak (*Kennedy* t. *Verenigd Koninkrijk*, EHRM 18 mei 2010, nr. 26839/05, par. 155).

Voorzienbaarheid van surveillance van juridische consultatie

3. Hoewel heimelijke surveillance van vertrouwelijke gesprekken tussen advocaten en cliënten onder uitzonderlijke omstandigheden wettelijk is toegestaan in het Verenigd Koninkrijk, gaat de kern van dit arrest over de vraag of de waarborgen hiervoor de privacytoets van art. 8, tweede lid, EVRM kunnen doorstaan. Sinds 2006 weten advocaten in Noord-Ierland dat hun gesprekken met gearresteerde cliënten afgeluisterd kunnen worden. Daarom vragen zij altijd aan de *Police Service of Northern Ireland* een garantie dat dit niet gebeurt. Als ze dit niet krijgen, zoals het geval was in deze zaak, dan stappen ze naar de rechter (par. 6-7). Volgens het Verenigd Koninkrijk zou de inmenging in deze zaak als rechtmatig moeten worden beschouwd (het staande Britse beleid is dat surveillance op basis van RIPA nog ontkend nog bevestigd wordt). Zelfs als dit niet zo zou zijn en er dus wel sprake zou zijn van inmenging, dan waren er adequate wettelijke waarborgen waaronder de voorzienbaarheid van het type surveillance (*intrusive* - of *directed*) dat plaatsvindt (sectie 26 RIPA). Voorzienbaarheid houdt in dat het voor burgers voldoende duidelijk en precies moet zijn omschreven onder welke omstandigheden een inbreuk op hun privacy kan worden gemaakt (zie bijv. *Weber en Saravia* t. *Duitsland*, EHRM 29 juni 2006, nr. 54934/00, «EHRC» 2007/13 m.nt. Loof). Voorzienbaarheid van communicatiesurveillance is van groot maatschappelijk belang. Naar aanleiding van de onthullingen van Edward Snowden speelt het gebrek aan transparantie over het bestaan en de procedures rondom de inzet van (massale) communicatiesurveillance door inlichtingen- en veiligheidsdiensten en de politie een belangrijke rol in politieke debatten over hervormingen van interceptie - en surveillancebevoegdheden.

4. De Britse Staat was in de zaak *R.E.* t. *Verenigd Koninkrijk* van mening dat de inmenging voorzienbaar was. Bovendien ging het volgens hen om gewone, *directed*, en niet om *intrusive surveillance*, dat minder zware waarborgen kent. Ook was er volgens de Britse Staat geen sprake van willekeurige inmenging (Sectie 26 RIPA / par. 109-110/126). Echter een eerdere uitspraak door het *House of Lords*, toen de hoogste Engelse rechterlijke instantie (nu het Hooggerechtshof), suggereerde dat de onderschepping van de vertrouwelijke advocaat-cliënt-relatie altijd als *intrusive surveillance* dient te worden beschouwd (House of Lords, *Re Mce* (Northern Ireland), UKHL 15, 2009, par. 38). Althans als RIPA de wettelijke basis vormt. Het was daarom niet ondenkbaar geweest dat deze *House of Lords*-uitspraak ook analoog van toepassing was verklaard door het EHRM op *R.E.* t. *Verenigd Koninkrijk*. Daarmee zou het sterkere waarborgregime van *intrusive surveillance* van toepassing worden verklaard. Echter het EHRM oordeelde dat niet het type interventie centraal dient te staan bij de afweging of er voldoende sterke waarborgen waren voor het beschermen van de informatie die is verkregen bij het heimelijk observeren of monitoren van de juridische consultaties tussen de klager en zijn advocaat, maar de mate van inmenging in een iemands privéleven (par. 141). Daarmee onderstreept de uitspraak in *R.E.* t. *Verenigd Koninkrijk* het belang van techniekonafhankelijke waarborgen voor communicatiesurveillance en -interceptie.

5. Verder, verwijzend naar de *Kennedy*-uitspraak (reeds aangehaald) oordeelde het EHRM dat ondanks dat de Britse wet- en regelgeving voldoende helder en dus

voorzienbaar is over bij welke strafbare feiten en personen *intrusive surveillance* is toegestaan en de autorisatieprocedure qua duur, de selectie van de relevante persoon en de maatregelen rondom voortzetting en beëindiging volstaat, er onvoldoende waarborgen waren voor de duur, het gebruik en de opslag van de geïntercepteerde - of geobserveerde informatie, voor het delen van de informatie met derden en de omstandigheden waarin informatie wordt vernietigd (Deel II van RIPA 'RIPA II'-regime, *Covert Surveillance Code of Practices*; par. 125, 133 en 138-141); *Kennedy* (reeds aangehaald), par. 155). *Kennedy* ging over de interceptie van telefoongesprekken tussen een advocaat en een cliënt, maar het EHRM past dit arrest analoog toe op het monitoren van vertrouwelijke gesprekken tussen advocaten en gedetineerde cliënten (zie ook *Bykov* t. *Rusland*, EHRM 10 maart 2009 (GK), nr. 4378/02 «EHRC» 2009/69 m.nt. Ölçer, par. 78). Daarmee onderschrijft zij, net als in eerdere uitspraken, dat art. 8 EVRM de privécommunicatie en correspondentie tussen advocaten en cliënten met krachtige extra waarborgen, waaronder tegen willekeurige inmenging, dient te worden beschermd (zie o.a. *Iordachi e.a*. t. *Moldavië*, EHRM 10 februari 2009, nr. 25198/02, par. 40).

6. Eigenlijk wordt de vraag of advocaten überhaupt hun werk goed kunnen doen als hun juridische consultaties niet vertrouwelijk zijn, niet echt beantwoord in deze zaak. Er wordt simpelweg verwezen naar eerdere jurisprudentie en het feit dat het heimelijk observeren en monitoren van juridische consultaties een zeer zware inmenging betreft (par. 131; *Michaud* t. *Frankrijk*, EHRM 6 december 2012, nr. 12323/11, «EHRC» 2013/91 m.nt. Ölçer, par. 118). De discussie over de positie van verschoningsgerechtigden laaide onlangs ook op bij Europese debatten over de hervormingen van de surveillance- en interceptiebevoegdheden van de inlichtingen- en veiligheidsdiensten en de politie. Zowel in Nederland als in het Verenigd Koninkrijk staan er wetsvoorstellen met uitgebreidere surveillance- en interceptiebevoegdheden op de rol. In het Engelse wetsvoorstel uit 2015, de *Investigatory Powers Bill*, dat uiteindelijk de RIPA dient te vervangen, staan er vrij algemene waarborgen voor vertrouwelijke communicatie tussen advocaten en cliënten. De voorgestelde waarborgen zouden generiek moeten gaan gelden voor speciale groepen zoals advocaten, journalisten, dokters en parlementariërs (Memorie van Toelichting wetsvoorstel *Investigatory Powers Bill*, 4 november 2015, p. 27-28, op: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf). Vanuit een mensenrechtenperspectief zijn er echter grote verschillen te identificeren tussen deze speciale groepen verschoningsgerechtigden. Door dit in lagere regelgeving, '*Codes*', vast te leggen, ondermijnt het wetsvoorstel een krachtig waarborgenstelsel. Immers regelgeving is gemakkelijker te wijzigen dan wetgeving. Dit terwijl in Nederland in het wetsvoorstel de Wet op de inlichtingen- en veiligheidsdiensten 20xx, alleen journalisten als verschoningsgerechtigden worden genoemd en de advocaten geheel buiten beschouwing worden gelaten (het Voorstel van wet; de Wet op de inlichtingen- en veiligheidsdiensten 20XX (consultatieversie juni 2015); College Rechten van de Mens (CRVDM), *Advies Concept Wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20..*, CRVDM, Utrecht, 31 augustus 2015, p.13-14). Dit is opmerkelijk: zeker in het kader van de recente uitspraak van het Gerechtshof Den Haag, dat oordeelde in een kort geding aangespannen door verschillende advocaten tegen de Staat der Nederlanden, dat de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) moeten

ophouden met het afluisteren van advocaten, tenzij er een wettelijke waarborg komt in de vorm van onafhankelijk toezicht vooraf (Hof Den Haag, 27 oktober 2015, nr. ECLI:NL:GHDHA:2015:2881). Daarom zou deze EHRM-uitspraak ook een rol kunnen gaan spelen in politieke debatten over de vertrouwelijke advocaat-cliënt-consultatie in de context van communicatiesurveillance en - interceptie. Immers één van de argumenten van bijvoorbeeld de Nederlandse wetgever bij de hervormingen van surveillance- en interceptiebevoegdheden, is dat de wet EVRM-proof moet zijn (zie het Voorstel van wet; de Wet op de inlichtingen- en veiligheidsdiensten 20XX, memorie van toelichting (consultatieversie juni 2015), p.200). Echter de vraag is, of dat gezien deze uitspraak nog geldt voor de Britse en Nederlandse wetsvoorstellen.

Noodzakelijk in een democratische samenleving?

6. Een tweede onderdeel van de uitspraak is, of de noodzaak van de heimelijke inmenging in de vertrouwelijke gesprekken tussen de klager en zijn advocaat een legitiem doel diende. Dit wordt vaak tegelijk getoetst met de voorzienbaarheidseis (*Kennedy* (reeds aangehaald), par. 119, 122, 155). Net als in het EHRM-arrest *Weber en Saravia* (reeds aangehaald) wordt de noodzaak van de inmenging beschouwd op basis van de vraag of er een legitiem doel is voor het onderscheppen van communicatie. Dit gaat dan concreet om een toets of de minimumeisen om willekeurige inmenging te voorkomen in de wet staan en publiekelijk bekend zijn (*Weber en Saravia* (reeds aangehaald) par. 95; *Valenzuela-Contreras* t. *Spanje*, EHRM 30 juli 1998, nr. 27671/95, par. 59). Zoals eerder genoemd, waren er volgens het EHRM in deze zaak onvoldoende waarborgen voor de duur, het gebruik en de opslag van de verkregen informatie, voor het delen van de informatie met derden en de omstandigheden waarin informatie wordt vernietigd en daarom was dit niet het geval. Als gevolg daarvan kan de noodzaak voor de inmenging op de juridische consultatie tussen een advocaat en zijn cliënt door middel van heimelijke surveillance in een democratische samenleving onvoldoende worden aangetoond. Dit is het geval ondanks het feit dat het in de *Valenzuela-Contreras*-uitspraak (reeds aangehaald) ging over de interceptie van communicatie en niet om surveillance. Echter zoals eerder gezegd, dient niet het type interventie centraal te staan in de toetsing of een inbreuk geoorloofd is of niet, maar de specifieke omstandigheden van de zaak en de mate van inmenging in iemands privéleven (par. 127).

Conclusie

7. De uitspraak *R.E.* t. *Verenigd Koninkrijk* is belangrijk omdat het EHRM wederom bevestigt dat de privacywaarborgen voor de heimelijke surveillance van vertrouwelijke gesprekken tussen advocaten en (gedetineerde) cliënten zeer sterk dienen te zijn. Een inmenging in de privécommunicatie vereist niet alleen dat helder moet zijn om welke strafbare feiten het gaat en op welke personen de surveillance van toepassing is, dat de autorisatieprocedure op orde moet zijn en de maatregelen rondom voortzetting en beëindiging volstaan, maar dat aan de waarborgen voor gebruik, de termijn van opslag, vernietiging en het delen van informatie minstens net zo veel waarde dient te worden gehecht. Daarmee laat het EHRM net als in haar recente uitspraak *Roman Zakharov* t. *Rusland* doorschemeren dat in het post-Snowden tijdperk het juridisch raamwerk rondom geheime surveillance van personen op orde moet zijn (*Roman Zakharov* t. *Rusland*, EHRM, 4 december 2015, nr. 47143/06). Ook moet informatie verkegen door de inzet van communicatiesurveillance door inlichtingen- en veiligheidsdiensten en de

politie niet zomaar nationaal – of internationaal – worden gedeeld. Met andere woorden, door te hameren op doelbinding, rekenschap en toezicht voor de geïntercepteerde informatie neemt het EHRM stelling in het debat rondom de neveneffecten van (massa-) surveillance in Europa. Hopelijk gaan staten nu werk maken van het creëren van sterkere waarborgen ter compensatie van inmenging op vertrouwelijke advocaat-cliënt-gesprekken.

mr. dr. Q. Eijkman, Hogeschool Utrecht / Universiteit Leiden