EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

Information Note on the Court's case-law 221

August-September 2018

Big Brother Watch and Others v. the United Kingdom - 58170/13, 62322/14 and 24960/15

Judgment 13.9.2018 [Section I]

Article 35

Article 35-1

Exhaustion of domestic remedies

Effective domestic remedy

Effectiveness of complaint about the general Convention compliance of a surveillance regime to the Investigatory Powers Tribunal: *admissible*

Article 8

Article 8-1

Respect for private life

Convention compliance of secret surveillance regime including the bulk interception of external communications: *violations*

Article 10

Article 10-1

Freedom of expression

Insufficient protection of confidential journalist material under electronic surveillance schemes: *violations*

Facts – The applicants, a number of companies, charities, organisations and individuals made up of three applications to the Court, complained about the scope and magnitude of the electronic surveillance programmes operated by the Government of the United Kingdom. The applicants all believed that due to the nature of their activities, their electronic communications were likely to have either been intercepted by the United Kingdom intelligence services; obtained by the United Kingdom intelligence services after being intercepted by foreign governments; and/or obtained by the United Kingdom authorities from Communications Service Providers (CSPs).

The applicants complained about the Article 8 compatibility of three discrete regimes: the regime for the bulk interception of communications under section 8(4) of the Regulation of Investigatory Powers Act (RIPA); the intelligence sharing regime; and the regime for the acquisition of communications data under Chapter II of RIPA.

The applicants in the third of the joined cases each lodged a complaint before the Investigatory Powers Tribunal (IPT) alleging violations of Articles 8, 10 and 14 of the Convention. As regards interceptions of external communications pursuant to a warrant issued under section 8(4) of RIPA, the IPT found that the regime and safeguards were sufficiently compliant with the requirements the European Court had laid down in *Weber and Saravia v. Germany* (dec.) for the interference to be "in accordance with the law" for the purposes of Article 8 of the Convention. It did, however, find two "technical" breaches of Article 8 concerning in one instance the retention for longer than permitted of lawfully intercepted material and in the other a failure to follow the proper selection-for-examination procedure. The applicants in the first and second of the joined cases did not bring complaints before the IPT.

Law

Article 35 (*exhaustion of domestic remedies*): The IPT was a specialist tribunal with sole jurisdiction to hear allegations of wrongful interference with communications as a result of conduct covered by RIPA. It considered both the generic compliance of the relevant interception regime as well as the specific question whether the individual applicant's rights had, in fact, been breached. Those involved in the authorisation and execution of an intercept warrant were required to disclose to the IPT all the documents it might require, including documents relating to internal arrangements for processing data which could not be made public for reasons of national security, irrespective of whether those documents supported or undermined their defence. The IPT had discretion to hold oral hearings, in public, where possible, and, in closed proceedings, it could appoint Counsel to the Tribunal to make submissions on behalf of claimants who could not be represented. When it determined a complaint, the IPT had the power to award compensation and make any other order it saw fit, including quashing or cancelling any warrant and requiring the destruction of any records. In considering the complaint brought by the applicants in the third of the joined cases, the IPT used all of those powers for the benefit of the applicants.

In view both of the manner in which the IPT had exercised its powers in the past fifteen years and the very real impact its judgments had had on domestic law and practice, the concerns expressed by the Court in *Kennedy v. the United Kingdom* about its effectiveness as a remedy for complaints about the general compliance of a secret surveillance regime were no longer valid.

It appeared to the Court that where the IPT had found a surveillance regime to be incompatible with the Convention, the Government had ensured that any defects were rectified and dealt with. Therefore, while the evidence submitted by the Government might not yet have demonstrated the existence of a "binding obligation" requiring it to remedy any incompatibility identified by the IPT, the Court nevertheless accepted that the practice of giving effect to its findings on the incompatibility of domestic law with the Convention was sufficiently certain for it to be satisfied as to the effectiveness of the remedy.

However, the Court accepted that, at the time the applicants in the first and second of the joined cases introduced their applications, they could not be faulted for having relied on *Kennedy* as authority for the proposition that the IPT was not an effective remedy for a complaint about the general Convention compliance of a surveillance regime. It therefore found that there existed special circumstances absolving those applicants from the requirement that they first bring their complaints to the IPT.

Article 8

(a) *The section 8(4) regime*

(i) *General principles relating to secret measures of surveillance, including the interception of communications* – In its case-law on the interception of communications in criminal investigations, the Court had developed the following six minimum requirements that had to be set out in law in order to avoid abuses of power: the nature of offences which might give rise to an interception order; a definition of the categories of people liable to have their communications intercepted; a limit on the duration of interception; 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 intercepted data may or must be erased or destroyed. In *Roman Zakharov v. Russia* [GC], the Court confirmed that the same six minimum requirements also applied in cases where the interception was for reasons of national security; however, in determining whether the impugned legislation was in breach of Article 8, it also had to have regard to the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law.

Review and supervision of secret surveillance measures might come into play at three stages: when the surveillance was first ordered, while it was being carried out, or after it had been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictated that not only the surveillance itself but the accompanying review should be effected without the individual's knowledge. Consequently, since the individual would necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it was essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In a field where abuse was potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it was in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure.

As regards the third stage, after the surveillance had been terminated, the question of subsequent notification of surveillance measures was inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers. There was in principle little scope for recourse to the courts by the individual concerned unless the latter was advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively or, in the alternative, unless any person who suspected that he or she had been subject to surveillance could apply to courts, whose jurisdiction did not depend on notification to the surveillance subject of the measures taken.

(ii) *The test to be applied* – The Court rejected the applicants' argument that the six minimum requirements should be "updated" by including requirements for objective evidence of reasonable suspicion in relation to the persons for whom data was being sought, prior independent judicial authorisation of interception warrants, and the subsequent notifications of the surveillance subject.

It was clear that bulk interception was a valuable means to achieve the legitimate aims pursued, particularly given the current threat level from both global terrorism and serious crime. Bulk interception was by definition untargeted, and to require "reasonable suspicion" would render the operation of such a scheme impossible. Similarly, the requirement of "subsequent notification" assumed the existence of clearly defined surveillance targets, which was simply not the case in a bulk interception regime. While the Court considered judicial authorisation to be an important safeguard, and perhaps even "best practice", by itself it could neither be necessary nor sufficient to ensure compliance with Article 8 of the Convention. Rather, regard had to be had to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse.

Accordingly, the Court would examine the justification for any interference by reference to the six minimum requirements, adapting them where necessary to reflect the operation of a bulk interception regime. It would also have regard to the additional relevant factors which it had identified in *Roman Zakharov*.

(iii) *The scope of application of secret surveillance measures* – In addressing the first two minimum requirements, the Court considered that the relevant legal provision was sufficiently clear, giving citizens an adequate indication of the circumstances in which and the conditions on which a section 8(4) warrant might be issued. There was no evidence to suggest that the Secretary of State was authorising warrants without due and proper consideration. The authorisation procedure was subject to independent oversight and the IPT had extensive jurisdiction to examine any complaint of unlawful interception. The Court accepted that the provisions on the duration and renewal of interception warrants, the provisions relating to the storing, accessing, examining and using intercepted data, the provisions on the procedure to be followed for communicating the intercepted data to other parties and the provisions on the erasure and destruction of intercept material were sufficiently clear as to provide adequate safeguards against abuse.

With regard to the selection of communications for examination, once communications had been intercepted and filtered, those not discarded in near real-time were further searched; in the first instance by the automatic application, by computer, of simple selectors (such as email addresses or telephone numbers) and initial search criteria, and subsequently by the use of complex searches. Selectors and search criteria did not need to be made public; nor did they necessarily need to be listed in the warrant ordering interception. Nevertheless, the search criteria and selectors used to filter intercepted communications should be subject to independent oversight; a safeguard which appeared to be absent in the section 8(4) regime. In practice the only independent oversight of the process of filtering and selecting intercept data for examination was the *post factum* audit by the Interception of Communications Commissioner and, should an application be made to it, the IPT. In a bulk interception regime, where the discretion to intercept was not significantly curtailed by the terms of the warrant, the safeguards applicable at the filtering and selecting for examination stage had to necessarily be more robust.

The Court was satisfied that the intelligence services of the United Kingdom took their Convention obligations seriously and were not abusing their powers under section 8(4) of RIPA. Nevertheless, an examination of those powers had identified two principal areas of concern: first, the lack of oversight of the entire selection process, including the selection of bearers for interception, the selectors and search criteria for filtering intercepted communications, and the selection of material for examination by an analyst; and secondly, the absence of any real safeguards applicable to the selection of related communications data for examination. In view of those shortcomings, the Court found that the section 8(4) regime did not meet the "quality of law" requirement and was incapable of keeping the "interference" to what was "necessary in a democratic society".

Conclusion: violation (five votes to two).

(b) *The intelligence sharing regime* – This was the first time that the Court had been asked to consider the Convention compliance of an intelligence sharing regime. The interference in the case had not been occasioned by the interception of communications itself but lay in the receipt of the intercepted material and subsequent storage, examination and use by the intelligence services of the respondent State. The circumstances in which intercept material could be requested from foreign intelligence services had to be set out in domestic law in order to avoid abuses of power. While the circumstances in which such a request could be made might not be identical to the

circumstances in which the State might carry out interception itself, they must nevertheless be circumscribed sufficiently to prevent – insofar as possible – States from using that power to circumvent either domestic law or their Convention obligations.

The Court was satisfied that there was a basis in law for the requesting of intelligence from foreign intelligence agencies, that that law was sufficiently accessible and pursued several legitimate aims. Furthermore, the Court considered the relevant domestic law and code indicated with sufficient clarity the procedure for requesting either interception or the conveyance of intercept material from foreign intelligence agencies. There was no evidence of any significant shortcomings in the application and operation of the regime.

Conclusion: no violation (five votes to two).

(c) *The Chapter II Regime* – The Chapter II regime permitted certain public authorities to acquire communications data from Communication Service Providers (CSPs). Domestic law, as interpreted by the domestic authorities in light of judgments of the Court of Justice of the European Union (CJEU), required that any regime permitting the authorities to access data retained by CSPs limited access to the purpose of combating "serious crime", and that access be subject to prior review by a court or independent administrative body. As the Chapter II regime permitted access to retained data for the purpose of combating crime (rather than "serious crime") and, save for where access was sought for the purpose of determining a journalist's source, it was not subject to prior review by a court or independent administrative body, it could not be in accordance with the law within the meaning of Article 8 of the Convention.

Conclusion: violation (six votes to one).

Article 10: The applicants in the second of the joined cases, a journalist and a newsgathering organisation, complained about the interference with confidential journalistic material occasioned by the operation of both the section 8(4) and the Chapter II regimes.

(a) *The section 8(4) regime* – The surveillance measures under the section 8(4) regime were not aimed at monitoring journalists or uncovering journalistic sources. Generally the authorities would only know when examining the intercepted communications if a journalist's communications had been intercepted. The interception of such communications could not, by itself, be characterised as a particularly serious interference with freedom of expression. However, the interference would be greater should those communications be selected for examination and would only be "justified by an overriding requirement in the public interest" if accompanied by sufficient safeguards relating both to the circumstances in which they might be selected intentionally for examination, and to the protection of confidentiality where they had been selected, either intentionally or otherwise, for examination.

It was of particular concern that there were no requirements either circumscribing the intelligence services' power to search for confidential journalistic or other material (for example, by using a journalist's email address as a selector), or requiring analysts, in selecting material for examination, to give any particular consideration to whether such material was or might be involved. Consequently, it would appear that analysts could search and examine without restriction both the content and the related communications data of those intercepted communications.

In view of the potential chilling effect that any perceived interference with the confidentiality of their communications and, in particular, their sources might have on the freedom of the press and, in the absence of any published arrangements limiting the intelligence services' ability to search and examine such material other than where "it

was justified by an overriding requirement in the public interest", the Court found that there had been a violation of Article 10 of the Convention.

(b) *The Chapter II Regime* – In considering the applicants' Article 8 complaint, the Court had concluded that the Chapter II regime was not in accordance with the law as it permitted access to retained data for the purpose of combating crime (rather than "serious crime") and, save for where access was sought for the purpose of determining a journalist's source, it was not subject to prior review by a court or independent administrative body.

The Court acknowledged that the Chapter II regime afforded enhanced protection where data was sought for the purpose of identifying a journalist's source. Nevertheless, those provisions only applied where the purpose of the application was to determine a source; they did not, therefore, apply in every case where there was a request for the communications data of a journalist, or where such collateral intrusion was likely. Furthermore, in cases concerning access to a journalist's communications data there were no special provisions restricting access to the purpose of combating "serious crime". Consequently, the Court considered that the regime could not be "in accordance with the law" for the purpose of the Article 10 complaint.

Conclusion: violations (six votes to one).

The Court also rejected the complaints under Article 6 and Article 14 combined with Articles 8 and 10 of the Convention as manifestly ill-founded.

Article 41: no claim made in respect of damage.

(See *Weber and Saravia v. Germany* (dec.), 54934/00, 29 June 2006, Information Note 88; *Kennedy v. the United Kingdom*, 26839/05, 18 May 2010, Information Note 130; *Roman Zakharov v. Russia* [GC], 47143/06, 4 December 2015, Information Note 191; see also *Liberty and Others v. the United Kingdom*, 58243/00, 1 July 2008, Information Note 110; *Malone v. the United Kingdom,* 8691/79, 2 August 1984; *Ben Faiza v. France* (dec.), 31446/12, 8 February 2018)
