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

Information Note on the Court's case-law 251

May 2021

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

Judgment 25.5.2021 [GC]

Article 8

Article 8-1

Respect for private life

Convention compliance of secret surveillance regime including bulk interception of communications and intelligence sharing: *violation, no violation*

Article 10

Article 10-1

Freedom of expression

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

[This summary also covers the judgment in *Centrum för rättvisa v. Sweden* [GC], no. 35252/08, 25 May 2021]

Facts – In *Big Brother Watch and Others,* the applicants, legal and natural persons, complained about the scope and magnitude of the electronic surveillance programmes operated by the Government of the United Kingdom. In a judgment of 13 September 2018 (see Information Note 221), the Chamber found that the bulk interception regime under section 8(4) of the Regulation of Investigatory Powers Act (RIPA) and regime for obtaining data from communications service providers under Chapter II of RIPA had violated Articles 8 and 10. It found no violation of Article 8 in respect of the intelligence sharing regime.

In *Centrum För Rättvisa*, the applicant, a non-governmental organisation, considers that there is a risk that its communications through mobile telephones and mobile broadband have been or will be intercepted and examined by way of signals intelligence. In Sweden, the National Defence Radio Establishment ("FRA") is authorised to conduct signals intelligence through bulk interception of communications. In a judgment of 19 June 2018 (see Information Note 219), a Chamber of the Court unanimously found no violation of Article 8.

The cases were referred to the Grand Chamber at the applicants' request.

Law –

The bulk interception of communications –

Article 8:

(i) *Interference* – Article 8 applied at each stage of the bulk interception process, and the degree of interference with privacy rights increased as the process moved through the different stages, notably: 1) interception and initial retention of communications and related communications data; 2) application of specific selectors to the retained communications/related communications data; 3) examination of selected communications/related communications data by analysts; and 4) subsequent retention of data and use of the "final product", including the sharing of data with third parties.

(ii) *Whether there was a need to develop the case-law* – In *Weber and Saravia* and *Liberty and Others*, the Court had applied the minimum safeguards developed in its case-law on targeted interception. However, seen in the light of the intervening technological developments, the scope of the surveillance activity considered in those cases would have been much narrower. More importantly, the Court had not expressly addressed the fact that targeted interception and bulk interception were different in a number of important respects. Unlike targeted interception, bulk interception was generally directed at international communications and predominantly used for foreign intelligence gathering and the identification of new threats from both known and unknown actors. Where specified individuals were "targeted", their devices were not monitored; rather, strong selectors were applied to the communications intercepted in bulk by the intelligence services.

(iii) *The test to be applied to bulk interception regimes* – While the safeguards already identified by the Court in the area of targeted interception regimes provided a useful framework, they had to be adapted to reflect the specific features of a bulk interception regime, the purpose of which was in principle preventive, rather that for the investigation of a specific target or an identifiable criminal offence. For instance, the requirement to define clearly in domestic law the categories of people liable to have their communications intercepted and the nature of offences which might give rise to such an order was not readily applicable to a bulk interception regime; nor was the requirement of "reasonable suspicion". Nevertheless, it was imperative that the domestic law should set out with sufficient clarity and detail the grounds upon which bulk interception might be authorised and the circumstances in which an individual's communications might be intercepted. Furthermore, in the context of bulk interception, the importance of supervision and review would be amplified, because of the inherent risk of abuse and the legitimate need for secrecy. Account also had to be taken of the increasing degrees of intrusion into the Article 8 rights of individuals as the bulk interception operation moved through the stages identified, which meant that the need for safeguards would be at its highest at the end of the process, where information about a particular person would be analysed or the content of the communications was being examined by an analyst. Therefore, process had to be subject to "end-to-end safeguards", meaning that, at the domestic level, an assessment had to be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception had to be subject to independent authorisation at the outset, when the object and scope of the operation were being defined; and that the operation had to be subject to supervision and independent *ex post facto* review. These were fundamental safeguards which would be the cornerstone of any Article 8 complaint bulk interception regime.

The Court was not persuaded that the acquisition of related communications data through bulk interception was necessarily less intrusive than the acquisition of content. Therefore, the interception, retention and searching of related communications had to be analysed by reference to the same safeguards as those applicable to content.

When conducting a global assessment of the operation of the regime, the Court would focus primarily on whether the domestic legal framework contained sufficient guarantees against abuse and whether the process was subject to "end-to-end safeguards". In doing so, it would have regard 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. In assessing whether the respondent State had acted within its narrower margin of appreciation, the Court needed to take account of a wider range of criteria than the six *Weber* safeguards. In addressing jointly "in accordance with the law" and "necessity", the Court would examine whether the domestic legal framework clearly defined:

1. The grounds on which bulk interception might be authorised;

In principle, the wider the grounds were, the greater the potential for abuse. However, narrower and/or more tightly defined grounds would only provide an effective guarantee against abuse if there were sufficient other safeguards in place to ensure that bulk interception was only authorised for a permitted ground and that it was necessary and proportionate for that purpose. The closely related issue of whether there existed sufficient guarantees to ensure that the interception was necessary or justified was therefore as important as the degree of precision with which the grounds on which authorisation might be given are defined. Consequently, in the Court's view, a regime which permitted bulk interception to be ordered on relatively wide grounds might still comply with Article 8 of the Convention, provided that, when viewed as a whole, sufficient guarantees against abuse were built into the system to compensate for that weakness.

2. The circumstances in which an individual's communications might be intercepted;

3. The procedure to be followed for granting authorisation;

Bulk interception had to be authorised by a body independent of the executive, although not necessarily a judicial one. That body had to be informed of both the purpose of the interception and the bearers or communication routes likely to be intercepted. That would enable them to assess the necessity and proportionality of the bulk interception operation and the selection of bearers.

The use of selectors – and strong selectors in particular – was one of the most important steps in the bulk interception process, as this was the point at which the communications of a particular individual might be targeted by the intelligence services. The Court accepted that the inclusion of all selectors in the authorisation might not be feasible in practice. Nevertheless, the authorisation had to at the very least identify the types or categories of selectors to be used. Moreover, enhanced safeguards had to be in place when strong selectors linked to identifiable individuals were employed by the intelligence services. The use of every such selector had to be justified – with regard to the principles of necessity and proportionality – by the intelligence services and that justification had to be scrupulously recorded and subject to a process of prior internal authorisation providing for separate and objective verification.

4. The procedures to be followed for selecting, examining and using intercept material;

5. The precautions to be taken when communicating the material to other parties;

The transmission by a Contracting State to foreign States or international organisations of material obtained by bulk interception had to be limited to such material as had been collected and stored in a Convention compliant manner and had to be subject to certain additional specific safeguards pertaining to the transfer itself: 1) the circumstances in which such a transfer might take place had to be set out clearly in domestic law; 2) the

transferring State had to ensure that the receiving State, in handling the data, had in place safeguards capable of preventing abuse and disproportionate interference (in particular, guaranteeing secure storage and restricting onward disclosure of the material). That did not necessarily mean that the receiving State had to have comparable protection to that of the transferring State, nor did it necessarily require that an assurance was given prior to every transfer; 3) heightened safeguards would be necessary when it was clear that material requiring special confidentiality – such as confidential journalistic material – was being transferred; and 4) the transfer of material to foreign intelligence partners also had to be subject to independent control.

6. The limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;

In *Centrum För Rättvisa,* while there had to be clear justification for special requirements regarding the destruction of material containing personal data, there also had to be a general legal rule governing the destruction of other material obtained through bulk interception of communications, where keeping it might affect, for example, the right of respect for correspondence under Article 8, including concerning legal persons. As a very minimum, there had to be a legal requirement to delete intercepted data that had lost pertinence for signals intelligence purposes.

7. The procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;

Each stage of the bulk interception process had also to be subject to a sufficiently robust supervision by an independent authority in a position to assess the necessity and proportionality of the action being taken, having due regard to the corresponding level of intrusion into the Convention rights of the persons likely to be affected. In order to facilitate this supervision, detailed records had to be kept by the intelligence services at each stage of the process.

8. The procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.

An effective remedy had to be available to anyone who suspected that his or her communications had been intercepted by the intelligence services, either to challenge the lawfulness of the suspected interception or the Convention compliance of the interception regime. As with targeted interception regimes, a remedy which did not depend on notification to the interception subject could also be an effective remedy in the context of bulk interception. In the absence of a notification requirement, it was imperative that the remedy be before a body which, while not necessarily judicial, was independent of the executive and ensured fairness of the proceedings, offering, in so far as possible, an adversarial process. The decisions of such authority had to be reasoned and legally binding.

(iii) *Assessment of the cases at hand* –

Centrum För Rättvisa v. Sweden – The Swedish bulk interception system was based on detailed legal rules, was clearly delimited in scope and provided for safeguards. The grounds upon which bulk interception could be authorised were clearly circumscribed, the circumstances in which communications might be intercepted and examined were set out with sufficient clarity, its duration was legally regulated and controlled and the procedures for selecting, examining and using intercepted material were accompanied by adequate safeguards against abuse. The same protections applied equally to the content of intercepted communications and communications data. Crucially, the judicial pre-authorisation procedure and the supervision exercised by an independent body served in principle to ensure the application of the domestic legal requirements and the

Convention standards in practice and to limit the risk of disproportionate consequences affecting Article 8 rights. Notably, regard had to be had to the fact that in Sweden the limits to be observed in each bulk interception mission, as well as its lawfulness and proportionality in general, were the subject matter of judicial pre-authorisation proceedings before the Foreign Intelligence Court, which sat in the presence of a privacy protection representative defending the public interest.

Nevertheless, the Court noted three shortcomings in the Swedish bulk interception regime. As regards the first of these shortcomings – the absence of a clear rule on destroying intercepted material which did not contain personal data – its potential for causing adverse consequences on Article 8 rights was limited by the fact that Swedish law provided for clear rules on the destruction of intercept material in a number of circumstances and, above all, when it contained personal data.

However, the second shortcoming – the absence of a statutory requirement to give consideration to the privacy interests of individuals when making a decision to transmit intelligence material to foreign partners – might potentially lead to very significant adverse consequences for affected individuals or organisations. It might allow information seriously compromising privacy rights or the right to respect for correspondence to be transmitted abroad mechanically, even if its intelligence value was very low. Such transmission might therefore generate clearly disproportionate risks for Article 8 rights. Furthermore, no legally binding obligation was imposed on the FRA to analyse and determine whether the foreign recipient of intelligence offered an acceptable minimum level of safeguards.

Finally, the third shortcoming consisted in the absence of an effective *ex post facto* review. Notably, the Foreign Intelligence Inspectorate's dual role and the absence of a possibility for members of the public to obtain reasoned decisions in some form in response to inquiries or complaints regarding bulk interception of communications weakened the *ex post facto* control mechanism to an extent that generated risks for the observance of the affected individuals' fundamental rights. Moreover, the lack of an effective review at the final stage of interception could not be reconciled with the Court's view that the degree of interference with individuals' Article 8 rights increased as the process advanced.

The above shortcomings were not sufficiently compensated by the existing safeguards. Therefore, the Swedish bulk interception regime overstepped the margin of appreciation left to the respondent State in that regard and, when viewed as a whole, did not contain sufficient "end-to-end" safeguards to provide adequate and effective guarantees against arbitrariness and the risk of abuse.

Conclusion: violation (fifteen votes to two).

Big Brother Watch and Others – When viewed as a whole, the regime, despite its safeguards, including some robust ones, had not contained sufficient "end-to-end" safeguards to provide adequate and effective guarantees against arbitrariness and the risk of abuse. In particular, the following fundamental deficiencies in the regime had been identified: the absence of independent authorisation, the failure to include the categories of selectors in the application for a warrant, and the failure to subject selectors linked to an individual to prior internal authorisation. Those weaknesses concerned not only the interception of the contents of communications but also the interception of related communications data. While the Interception of Communications Commissioner ("the IC Commissioner") provided independent and effective oversight of the regime, and the Investigatory Powers Tribunal ("IPT") offered a robust judicial remedy to anyone who suspected that his or her communications had been intercepted by the intelligence services, those important safeguards were not sufficient to counterbalance the above shortcomings. The bulk interception of communications regime

under section 8(4) of the Regulation of Investigatory Powers Act (RIPA) did not meet the "quality of law" requirement and was therefore incapable of keeping the "interference" to what was "necessary in a democratic society".

Conclusion: violation (unanimously).

Article 10 (Big Brother Watch and Others) –

(i) *Requisite safeguards* – Under the bulk interception regime, confidential journalist material could have been accessed by the intelligence services intentionally, through the deliberate use of selectors or search terms connected to a journalist or news organisation. As that situation would very likely result in the acquisition of significant amounts of confidential journalistic material, it could undermine the protection of sources to an even greater extent than an order to disclose a source; the interference would be commensurate with that occasioned by the search of a journalist's home or workplace. Therefore, before the intelligence services used selectors or search terms known to be connected to a journalist, or which would make the selection of confidential journalistic material for examination highly probable, the selectors or search terms had to be authorised by a judge or other independent and impartial decision-making body vested with the power to determine whether they had been "justified by an overriding requirement in the public interest" and, in particular, whether a less intrusive measure might have sufficed to serve the overriding public interest.

Confidential journalist material could also be accessed unintentionally, as a "bycatch" of the bulk interception operation; in such case, the degree of interference with journalistic communications and/or sources could not be predicted at the outset. In *Weber and Saravia*, the Court accepted that the initial interception, without examination of the intercepted material, did not constitute a serious interference with Article 10 of the Convention. Nevertheless, given that, owing to technological developments, surveillance which was not targeted directly at individuals had the capacity to have a very wide reach indeed, it was imperative that domestic law contained robust safeguards regarding the storage, examination, use, onward transmission and destruction of such confidential material. Moreover, if and when it became apparent that the communication or related communications data contained confidential journalistic material, their continued storage and examination by an analyst had to only be possible if authorised by a judge or other independent and impartial decision-making body vested with the power to determine whether continued storage and examination was "justified by an overriding requirement in the public interest".

(ii) *Application to the facts of the present case* – Some applicants were a newsgathering organisation and a journalist: the impugned regime, which had interfered with their right to freedom of expression, did not comply with the above requirements. The additional safeguards concerning the storage, onward transmission and destruction of confidential journalistic material did not address the weaknesses identified by the Court in its analysis of the regime under Article 8.

Conclusion: violation (unanimously).

Receipt of intelligence from foreign intelligence services (*Big Brother Watch and Others)* –

Article 8:

Where a request was made to a non-contracting State for intercept material, the request had to have a basis in domestic law, and that law had to be accessible to the person concerned and foreseeable as to its effects (see *Roman Zakharov v. Russia* [GC]). It was also necessary to have clear detailed rules which give citizens an adequate indication of

the circumstances in which and the conditions on which the authorities were empowered to make such a request and which provided effective guarantees against the use of that power to circumvent domestic law and/or the States' obligations under the Convention. Upon receipt of the material, the receiving State had to have in place adequate safeguards for its examination, use and storage; for its onward transmission; and for its erasure and destruction. Those safeguards, first developed by the Court in its case-law on the interception of communications by Contracting States, were equally applicable to the receipt, by a Contracting State, of solicited intercept material from a foreign intelligence service. If States did not always know whether the received material was the product of interception, then the same standards should apply to all received material that could be the product of intercept. Finally, any regime permitting the intelligence services to request either interception or intercept material from non-Contracting States, or to directly access such material, had to be subject to independent supervision, and there had also to be the possibility for independent *ex post facto* review.

The Court, limiting its examination to the complaint about the receipt of solicited intercept material from the US National Security Agency ("NSA"), was satisfied the those requirements had been fulfilled in the present case and that the regime for requesting and receiving intercept material had thus been compatible with Article 8.

Conclusion: no violation (twelve votes to five).

The Court also held, by twelve votes to five, that there had been no violation of Article 10 in respect of the receipt of intelligence from foreign intelligence services, as the complaint gave rise to no separate issue to that arising out of Article 8.

Acquisition of communications data from communications service providers (Big Brother Watch and Others) – The Court held, unanimously, that there had been a violation of Articles 8 and 10, as the operation of the regime under Chapter II of RIPA had not been "in accordance with the law".

Article 41 (both cases): no claim in respect of damage.

(See also *Weber and Saravia v. Germany* (dec.), 54934/00, 29 June 2006, Legal Summary; *Liberty and Others v. the United Kingdom*, 58243/00, 1 July 2008, Legal Summary; *Roman Zakharov v. Russia* [GC], 47143/06, 4 December 2015, Legal Summary)
