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

Third European Intelligence Oversight Conference:

National Security and the Role of Oversight Bodies in European Jurisprudence

Speech by Robert Spano

Rome, 7 October 2021

I. Introduction

I would like to thank very warmly the General Prosecutors' Office of the Court of Appeal of Rome, and in particular Mr. Antonio Mura, for inviting me to take part in this 3rd European Intelligence Oversight Conference. It is my great pleasure as President of the European Court of Human Rights to be here with you in Rome. I would like to salute the other speakers today and in particular Guido Raimondi, my friend, former colleague and President of the European Court of Human Rights.

The overriding theme for your discussions will be National Security and the Role of Oversight Bodies in European Jurisprudence. This is a technical and fast-moving area of the law, which has the power to impact greatly on individual rights and deserves our particular attention.

The focus of my intervention will be on the oversight requirements in relation to intelligence services as set out most recently in the two connected Grand Chamber judgments of the Court from May this year: *Big Brother Watch and Others*[1] and *Centrum för rättvisa*[2].

First three preliminary remarks.

The European Convention on Human Rights provides a set of minimum standards. Member States are of course free to take into account and put into place oversight recommendations from other sources of both hard and soft law which may lead to higher standards. Here I would mention the useful recommendations concerning the democratic oversight of security services adopted by the Venice Commission[3], the Parliamentary Assembly (PACE)[4] and the Commissioner for Human Rights[5].

Secondly, the precise oversight regime to be put in place is the choice of each Member State. The Court is not prescribing any one particular "ideal" model. To be Convention complaint the domestic legal framework must contain sufficient guarantees against abuse and the interception process

[1] *Big Brother Watch and Others v. the United Kingdom* [GC], nos. 58170/13 and 2 others, 25 May 2021
[2] *Centrum för rättvisa v. Sweden* [GC], no. 35252/08, 25 May 2021
[3] Report on the Democratic Oversight of Signals Intelligence Agencies, Adopted by the Venice Commissioner at its 102nd Plenary Session (Venice, 20-21 March 2015).
[4] PACE Recommendation 2067 (2015) on Mass Surveillance
[5] Democratic and effective oversight of national security services, Issue paper by the Commissioner for Human Rights, 2015.

should be subject to "end-to-end safeguards" (more of that later). The Court, if called upon to assess the regime in place, will take a global view of how it works as a whole.

Thirdly, the Court pays a great deal of attention to the work and specific findings of the national authorities and courts engaged in intelligence work. In the *Big Brother Watch and Others* case I will examine shortly, the Court refers to the judgments of the UK's Investigatory Powers Tribunal, the domestic oversight Commissioners and Intelligence and Security Committee of the Westminster Parliament. It also looked at relevant case-law of other national courts such as the judgment of the German Federal Constitutional Court of 19 May 2020 and the judgment of the Court of Appeal of The Hague of 14 March 2017. It also goes without saying that the Court looks closely at the relevant case-law of the Court of Justice of the European Union. These cross-references are an important part of our dialogue and the best way in which we can understand and balance the competing concerns at play. This comparative exercise is all the more relevant where large parts of intelligence gathering take place in secret.

You may be surprised to learn that the European Court of Human Rights has been dealing with complaints related to secret surveillance since the 1970s. Of course, the Edward Snowden revelations from 2013 on the extent of electronic surveillance programmes has brought the particular issue of mass surveillance to the attention of the general public and there are a number of compelling reasons why the digital age and the global Internet has brought about a paradigm shift in how we must accordingly ensure democratic oversight.

Let me set the scene by tracing briefly the evolution of the Court's case-law in relation to secret surveillance.

II. The evolution of the Court's case-law on secret surveillance

The right to personal data protection does not figure as an autonomous right in the European Convention on Human Rights. This is hardly surprising when one considers that the European Convention was adopted in 1950 and data protection laws at the domestic level emerged only in the 1970s. However, another Council of Europe instrument, Convention 108, specifically protects data protection rights This is the first, and to date, the only internationally legally binding instrument dealing with data protection. The Convention underwent a modernisation process in 2018, completed with the adoption of an amending Protocol.[6]

In parallel, the right to the personal protection of one's data under the European Convention on Human Rights has developed under the wide umbrella of Article 8 which guarantees the right to respect for private and family life, home and correspondence, and lays down the conditions under which restrictions of this right are permitted. Indeed, in recent case-law the Court has acknowledged that "*the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention*."[7]

The right to respect for private life is not an absolute right, but must be balanced against, and reconciled with, other legitimate interests and rights, be they of other persons (private interests) or of society as a whole (public interests).

---

[6] https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

[7] *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], no. 931/13, 27 June 2017

Early cases involving secret surveillance of citizens by their authorities concerned interceptions of letters, telegrams or telephone calls (telephone tapping).[8] Interferences were justified by governmental authorities on the basis of the prevention of terrorism or ordinary crime. Yet as early as in 1978, the Court found in *Klass v. Germany*, a case which involved an early type of non-targeted interception, that the exception in Article 8 § 2 was:

> *"to be narrowly interpreted. Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions."*

Further on in that case (§ 49), the Court stated that:

> *The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.*

In *Rotaru v. Romania*[9], where the facts went back to the early 1990s, the applicant complained about the Romanian Intelligence Service holding personal information on him in a file. The Court found that, while the domestic law allowed for the gathering, recording and archiving in secret files of information affecting national security, it did not lay down any limits on the exercise of those powers, which remained at the discretion of the authorities. The Court therefore concluded that the domestic law did not comply with the requirement of foreseeability under Article 8 of the Convention and that this article had been violated.

Let us now fast forward to some further examples of how the Court has responded to bulk interception. Here I am thinking of *Weber and Saravia v. Germany*[10] from 2006, a follow-up to *Klass v. Germany*, which concerned generalized "strategic monitoring" and *Liberty and Others v. the United Kingdom*[11] from 2008 which concerned a general interception of telephone, facsimile, e-mail and data communications. In *Weber and Saravia*, an inadmissibility decision, the Court underlined that:

> *"It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated …. The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (…)"*

In *Roman Zakharov v. Russia* [12] from 2015, the Court also had regard to the arrangements for supervising and reviewing the interception regime in place. It found that these measures should come into play at three stages: when the surveillance was first ordered, while it was being carried out, or after it had been terminated.

---

[8] *See for example: Klass and Others v. Germany, No. 5029/71* and *Malone v. the United Kingdom*, No. 8691/79, 2 August 1984.
[9] *Rotaru v. Romania [GC], no. 28341/95, ECHR 2000-V*
[10] *Weber and Saravia v. Germany* (dec.), no. 54934/00, ECHR 2006-X
[11] *Liberty and Others v. the United Kingdom*, no. 58243/00, July 2008
[12] *Roman Zakharov v. Russia* [GC], no. 47143/06, ECHR 2015

III. The safeguards as set out most recently by the Grand Chamber of the European Court

I now turn to discuss the two most recent judgments of the Grand Chamber of the European Court adopted on the same day in May this year: *Big Brother Watch and Others* and *Centrum för rättvisa*. Here the Court examined the Convention compliance of two different regulatory frameworks and set out updated requirements in relation to bulk interception. The legal approach in the two cases is identical, however the findings on the facts of each case differed.

The Grand Chamber considered that a number of factors warranted a fresh look at its own 2006 and 2008 case-law on bulk interceptions. Why?

Firstly, because technology has increased the volume of communications crossing the globe. Secondly, because the vast majority of communications now take digital form. Surveillance, when not targeted specifically at one person, has the capacity to have a very wide reach both inside and outside of the surveilling State. Thirdly, the threats being faced by Contracting States and their citizens have also proliferated, these include global terrorism, drug trafficking, human trafficking, the sexual exploitation of children and cybercrime.

In its judgments the Court accepted that bulk interceptions regimes are permissible under the Convention and set out the approach to be followed in bulk interception cases, which it distinguished from targeted interceptions for a number of reasons. Firstly, because bulk interceptions are generally directed at international communications (that is, communications physically travelling across State borders). Secondly, bulk interceptions are not as a rule used for the purposes of investigating crime, as was the case for targeted interceptions, but rather for the purposes of intelligence gathering, and the early detection of terrorist, cyber and other serious security threats.

In the context of bulk interception, the Court found that the importance of supervision and review would be amplified because of the inherent risk of abuse and because the schemes were often shrouded in secrecy.

Accordingly, to minimise the risks present the Court considered that the process must be subject to "end-to-end" safeguards, meaning that,

> *"at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review."*

In the Court's view the degree of interference with individuals' Article 8 rights increases as the process advances.

So what is required by the Court?

- At the outset an independent authority (not necessarily a judicial body) is required to assess the purpose of the interception, the selection of the bearers and the categories of the selectors taking into account the necessity and proportionality of the operation;

- During the execution of the interception order, an independent authority should supervise execution, including its renewals, the use, storage and onward transmission and deletion of obtained data, with detailed records being kept to facilitate this supervision;
- In the end an *ex post facto* review by an independent body (not necessarily judicial) which can ensure the fairness of proceedings offering in so far as possible an adversarial process. The decisions of the body should be reasoned and legally binding as to the cessation of the unlawful interception and the destruction of unlawfully obtained or stored material.

In assessing whether a bulk interception regime is Convention compliant the Court will conduct a *global* assessment of the operation of the regime – does the domestic legal framework contain sufficient guarantees against abuse? Is the process subject to "end-to-end safeguards"? The Court will examine whether the domestic legal framework meets the Court's requirements, and namely eight factors:

1. The grounds on which bulk interception may be authorised;
2. The circumstances in which an individual's communications may be intercepted;
3. The procedure to be followed for granting authorisation;
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;
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;
7. The procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance; and
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.

Now a word about the outward exchange of intercept data with foreign intelligence services. The Court noted that some States are regularly sharing material with their intelligence partners and even, in some instances, allowing those intelligence partners direct access to their own systems. While this practice is not prohibited as such by the Convention, the Court used the opportunity to make specific findings. The material shared should only be material collected and stored in a Convention compliant manner. Additional safeguards must be put in place pertaining to the transfer, as set out in the judgment.[13] With respect to receipt of information collected through bulk interception by partner non-member states, the Court held that "*the protection afforded by the Convention would be rendered nugatory if States could circumvent their Convention obligations by requesting either the interception of communications by, or the conveyance of intercepted communications from, non-Contracting States*". Thus, national law should provide in this respect "*effective guarantees against the use of this power to circumvent domestic law and/or the States' obligations under the Convention*".

Turning to the findings of the Court in the two specific cases, the Court examined the regulatory regimes in place in the United Kingdom and Sweden and found them both lacking but at different stages of the process. As regards the United Kingdom, the deficiencies were identified at the beginning of the process in terms of, *inter alia,* the absence of independent authorisation, the failure to include the categories of selectors in the application of the warrant, the failure to subject selectors linked to an individual to prior internal authorisation.

[13] See § 362 of *Big Brother Watch and Others v. the United Kingdom*.

For Sweden, the shortcomings were identified in the *ex post facto* review, in particular 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.

IV. Conclusion

The Court has recognised that bulk interception is of vital importance to Contracting States in identifying modern threats to their national security.

Yet the task for Member States is not an easy one. They must strive to find the right balance between our concept of freedom and our need for security.

Since its first case-law on the retention of secret paper files, the Court has been striving to find that balance and it is interesting to see how many of the general principles enunciated almost 50 years ago are still pertinent today.

In his concurring opinion in the case of *Malone v. the United Kingdom* from 1984, Judge Pettiti stated:

"The Court [acts as guardian of the Convention] by investing Article 8 with its full dimension and by limiting the margin of appreciation especially in those areas where the individual is more and more vulnerable as a result of modern technology; recognition of his right to be "left alone" is inherent in Article 8 (art. 8). The Convention protects the community of men; man in our times has a need to preserve his identity, to refuse the total transparency of society, to maintain the privacy of his personality."

This opinion still accurately encapsulates the importance of why privacy is worth defending.