OCTOPUS Conference 2016

Cooperation Against Cybercrime
16-18 November 2016
Palais de l'Europe, Strasbourg France

PLENARY
Human Rights and Rule of Law in Cyberspace: Threats and Safeguards

Judge Robert Spano
European Court of Human Rights

1. Ladies and gentlemen,

   It is a great honour and a pleasure to be invited to address you at this impressive conference dealing with one of the most important and complex issues facing modern criminal justice and intelligence systems today.

2. It cannot be disputed that cyberspace has transformed modern society, including the law. In almost all fields of law the advent of the Internet is influencing the development of existing legal principles and rules, including in the field of human rights law. Numerous conceptual and practical problems have in particular arisen in connection with the fundamental right to privacy, freedom of expression and the right to property.

3. The necessity of robust law enforcement and effective national security safeguards in the cyberspace era obviously implicates very important and difficult questions related to the very elusive balance to be struck between public interest imperatives, on the one hand, and fundamental human rights, on the other. In this area, as in others, the rule of law does not allow governments to adopt an ends justify the means mentality. But, law enforcement and national security authorities must nonetheless be given some flexibility to resort to measures that safeguard and protect people's lives, bodily and personal integrity and economic interests against criminal behaviour. It is the resolution of this tension between the public interest and individual rights which is the bread and butter work of the European Court of Human Rights, the case-law of which I have been asked to talk about here today.

4. In my brief intervention, I will proceed in two parts. First, I want to discuss some recent judgments of the Court in the field of mass surveillance activities interfering with the right to privacy under Article 8 and attempt to distil for you the main elements of this case-law. Second, on that basis and before I conclude, I will say a few words about whether the current case-law can be read to differentiate between

measures taken by criminal justice authorities, investigating specific crimes and securing specified data, and measures taken by services responsible for national security, which may include bulk interception for intelligence and preventive purposes.

5. Let me then turn to my first part. The case-law of the Strasbourg Court.

6. It is interesting to note at the outset that the Court has a rather long history of dealing with law enforcement and surveillance type activities, in particular in relation to terrorist threats facing the continent during different periods over the past few decades. In fact, one of the most famous and seminal cases from the so-called old Court, the one that was in place prior to 1998 when the current Court was established, is the case of *Klaas v Germany* of 1978 where the applicants, five German lawyers, complained in particular about legislation in Germany empowering the authorities to monitor their correspondence and telephone communications without obliging the authorities to inform them subsequently of the measures taken against them. The Court held that there had been no violation of Article 8 of the Convention, finding that the German legislature was justified in considering the interference as being necessary in a democratic society in the interests of national security and for the prevention of disorder or crime. However, the Court emphasised that powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as they are strictly necessary for safeguarding democratic institutions.

7. Fast-forwarding now almost forty years, the Grand Chamber of the Strasbourg Court delivered judgment in December of last year in the most recent landmark case dealing with the issue of mass targeted surveillance, the case of *Roman Zakharov v Russia*. The applicant in that case alleged that the system of secret interception of mobile telephone communications in Russia violated his right to respect for his private life and correspondence and that he did not have any effective remedy in that respect.

8. The Grand Chamber emphasised that review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. In examining further each of these stages, the Court based its reasoning on three fundamental principles:

   First, that “foreseeability” of the law in the context of communications interception cannot be conceptualised in the same way as it is in many other fields. However, to prevent arbitrariness, it is essential to have clear, detailed rules so as to give citizens an adequate indication as to the circumstances and the conditions in which public authorities are empowered to resort to any such measures.

   Second, the law must indicate with sufficient clarity the scope of discretion conferred on the competent authorities.

Third, the Court importantly for our purposes set out the minimum safeguards that should be set out in law in order to avoid abuse, namely:

one, the nature of the offences which may give rise to an interception order;
two, a definition of the categories of people liable to have their communications intercepted;
three, a limit on the duration of such monitoring;
four, the procedure to be followed for examining, using and storing the data obtained;
five, the precautions to be taken when communicating the data to other parties, and
six, the circumstances in which data may or must be erased or destroyed.

9. In finding a violation of Article 8 in the case, the Grand Chamber looked to all of these six elements on the basis of an *in abstracto* examination of the Russian law in question.

10. In a more recent Chamber judgment, delivered after *Roman Zakharov*, the case of *Szabó and Vissy v. Hungary*, the fact that virtually any individual in Hungary could be subjected to secret surveillance was of particular concern to the Court. It could not be ruled out that the broad-based provisions of the National Security Act could be used to enable strategic, large-scale interception, constituting a matter of serious concern.

11. In particular, the Hungarian legislation did not describe the categories of persons susceptible to communications interception. There was no requirement of any kind for the authorities to demonstrate the actual or presumed relation between the individuals concerned and the prevention of the supposed threat.

12. Given that the scope of the surveillance measures in Hungary extended to virtually all citizens, that the ordering took place entirely within the executive realm and without an assessment of strict necessity, that new technologies enabled the Government to intercept masses of data easily, and given the absence of any effective remedial measures, notably in the judicial sphere, the Court concluded that there had been a violation of Article 8 of the Convention.

14. Let me now then turn to my second part and make the following remarks before I conclude.

15. First, it is a recurrent and fundamental theme of the case-law of the Strasbourg Court that the nature and extent of the protections afforded by human rights provisions in the field of criminal justice and national security are primarily rule of law oriented. Now, what do I mean by this?

16. Usually when the Court deals with claims of a breach of Article 8 of the Convention, or of the other so-called qualified rights which allow for limitations, the Court undertakes a three step analysis of the interference in question. One, was

it prescribed by law, two, did it pursue a legitimate aim, and three, was it proportionate to the aim pursued, or in other words necessary in a democratic society. However, as explained by the Grand Chamber in *Roman Zakharov*, in cases where the legislation permitting these kinds of law enforcement surveillance type measures is being contested before the Court, the quality of the law and the proportionality steps of the analysis are merged so to speak. In other words, the legality requirement is also meant to ensure that surveillance measures are applied only when "necessary in a democratic society".

17. My second point concerns the question that I have been asked to comment on, that is whether the case-law of the Strasbourg Court can be read to differentiate between measures taken by criminal justice authorities, investigating specific crimes and securing specified data, and measures taken by services responsible for national security, which may include bulk interception for intelligence and preventive purposes.

18. Unfortunately, the answer to that question is not completely clear as the Court, at least at the Grand Chamber level, has not to date dealt in comprehensive terms with the latter category, although several interesting cases are pending, in particular from the United Kingdom.

19. I recall that the case of *Roman Zakharov v Russia* dealt mainly with secret surveillance measures for classical law enforcement/criminal justice type activity in the investigation of specific crimes and the collection of evidentiary data for those purposes. However, the case of *Szabo and Vissy v Hungary* does indeed implicate more general issues of national security type bulk collection of communications and it is clear from the reasoning in that case that the framework set out in *Roman Zakharov* forms the jurisprudential basis for its analysis in that context. Having said that, it is clear that the mass interception of data for pure preventive, intelligence type purposes, and not least its cross-border dissemination between intelligence authorities in different countries, presents to some extent a different paradigm in relation to the application of human rights principles than traditional criminal justice type activity. It remains to be seen whether the Court will consider it necessary to develop its case-law further to take account of that difference.

20. To conclude, as I have hopefully demonstrated in this brief intervention, the current case-law of the European Court of Human Rights demonstrates in my view that the core of the human rights protection afforded to the citizen when States are confronted with enforcing the law in cyberspace is decided by the domestic legislator when formulating and enacting legislation in this field. It is the norm of domestic law that provides both the required foreseeability and the basis for the examination of necessity. Therefore, it goes without saying that comprehensive policy making in this field in an international fora, like the Council of Europe, is of utmost importance as it can readily influence domestic legislators to

do their job in full cognisance of the need to balance individual human rights with the public interest through robust and effective law enforcement.