**Hearing of the ECHR in the cases of Mikolaj PIETRZAK and Dominika BYCHAWSKA- SINARSKA and others v. Poland**

**Oral submission - UN Special Rapporteur on the protection and promotion of human rights while countering terrorism**

Strasbourg, 27 September 2022

Mr. President, Distinguished members of the Court,

The disclaimer relating to UN privileges and immunities that was included at the beginning of the Amicus Brief submitted to this Court in relation to this case in 2020 applies in full to this oral submission.

The Special Rapporteur’s mandate intervention in this case arises because the case represents one example of the structural problem of the contemporary overuse of counter-terrorism powers and the serious human rights implications that follow.

In the mandate’s view, the right to privacy functions as a gateway right that protects and enables many other rights and freedoms, and its protection is intimately co-related to the existence and advancement of a democratic society. Therefore, the Special Rapporteur sees the escalation in the use of secret surveillance and the collection of content information and of metadata for countering terrorism purposes, combined with the bolting development of under-regulated new technologies, as a significant threat to democratic societies.

The scale of the intrusion and the lack of safeguards, even in countries with limited threats of terrorism, is a great concern. In this respect, we would like to bring to this Court’s attention that according to the Global Counter-Terrorism Index, which ranks all countries of the world and is used to evaluate a risk of terrorism, Poland holds the last position, along with several other countries identified as having a negligible threat of terrorism.

I will limit my remarks to three points, which we believe are of relevance to the follow-up questions that this Court has asked for this hearing.

1. **In accordance with the law**

The first point I will address today relates to the requirement that the interference with rights must be “in accordance with the law”. The mandate notes that the approach of the Court with respect to secret surveillance is to address jointly the “in accordance with the law” and the “necessity” requirements, which implies (1) that the domestic law must be accessible, foreseeable in its application, and that it ensures that secret surveillance measures are applied only when they are “necessary in a democratic society.”[[1]](#footnote-1)

This Court has also noted, in a recent case against Sweden, that even in the case of bulk interception, “domestic law should set out with sufficient clarity the grounds upon which bulk interception might be authorised and the circumstances in which an individual’s communications might be intercepted”.[[2]](#footnote-2)

This approach has both substantive and procedural consequences for the law.

**1.1 Substantive requirement: Definition of terrorism**

Turning to the substantive requirement in the Polish law, the starting point for any in-country engagement by the Mandate is always an assessment of the definitions used in national security legislation. We often find that definitions of terrorism are overly broad and vague and do not comply with the principle of legality, which implies that offences are defined with clear and precise provisions, so as to respect the principle of legal certainty and ensure that it is not subject to interpretation which would unduly broaden the scope of the proscribed conduct. For this Mandate, there is therefore a very strong link between the principle of legal certainty and the question of “in accordance with the law”.

According to the UN High Commissioner for Human Rights, “the nature of the offence and the category of persons that may be subjected to surveillance must be described. Vague and overbroad justifications (…) do not qualify as adequately clear laws”.[[3]](#footnote-3)

We note that the collection of content information in Poland is allowed under the Counter-Terrorism Law against “foreigners suspected of terrorist activity”. Article 20 of the Police Act allows the collection of metadata for the broad purposes of the “prevention or detection of crimes or in order to save human life and health”. Although not specifically referred to in the law, we understand this broad concept to include the objective of countering terrorism, which is often the primary reason put forward by States to adopt secret surveillance measures and collect metadata.

In this respect, we refer to the UN Human Rights Committee’s concerns,[[4]](#footnote-4) that the definition of “terrorist crime” in the Polish Penal Code is overly broad and does not adequately define the nature and the consequences of the act concerned. Moreover, the Committee found that the notion of “terrorist incident” in the Counter-Terrorism law is broad and imprecise. These concerns are shared by the Special Rapporteur.

The lack of clarity as to the definitions of terrorism carries two main risks.

One, that laws that refer to these terms directly or indirectly as the basis for the use of special powers – such as secret surveillance of content and the collection of metadata – can be applied to an overly broad range of persons. This point is even more resonant in the context of the use of such powers to prevent acts of terrorism, which involves applying such powers regarding possible future events.

Two, that because overly broad and vague definitions also give broad discretion to those in charge of using them, any control or review of the proportionality of their use is also, as a consequence, limited.

In sum, where the starting point of the application of special powers is ambiguous (such as an unclear definition of terrorism), there is scope for abuse of power. It is the view of the Mandate that the grounds upon which secret surveillance can be authorised must be very tightly and sufficiently circumscribed, particularly when the notion of terrorism is involved.

* 1. **Procedural safeguards**

Allow me now to turn to the issue of procedural safeguards. Given the well-trodden and demonstrated risks to the right to privacy as recognised by this Court,[[5]](#footnote-5) but also to fundamental freedoms, the mandate of the Special Rapporteur does not make a distinction between the secret collection and treatment of content information or of metadata.

In both cases, human rights compliance of the measures has to be assessed at every stage of data usage. This requires a number of safeguards, including judicial authorisation, effective remedies for violations, which cannot—given that the legislation can indiscriminately affect all users of communication services—exist without the third requirement, which is ex-post notification.

We would like to underscore the particular risks to freedom of expression posed by secret surveillance measures, which can have a serious impact on civil society organisations, lawyers and members of the opposition, and ultimately endanger the functioning of democratic societies as a whole. We note here that these actors are not entitled to absolute and in some cases even to limited protection under Polish law.

This highlights the importance of independent systemic oversight. We note that neither the Police Law (which only provides for a broad summary report absent obligatory review by a judge) nor the Counter-Terrorism legislation (which only provides for information to be provided absent obligatory assessment) include robust ex-post oversight and review mechanisms.

If such mechanisms existed, they should (1) assess human rights compliance in each case of use by the authorities of the exceptionally intrusive measures, but also (2) beyond individual cases, look at the overall systemic impact of the measures, including on certain specific categories of individuals.

1. **The targeting of foreigners under the counter-terrorism law**

Allow me to now turn to my last point, which relates to the collection of the content of communications against non-nationals suspected of terrorist activity, on the basis of an executive decision and with extremely limited control, as allowed by the Counter-Terrorism law. Given the broadness of these provisions, the comments made above are obviously highly relevant here.

We note that unless evidenced otherwise, the threat of terrorism can equally come from nationals and non-nationals, alike. Security measures that target only non-nationals have the result of not only failing adequately to address the threat of terrorism, but also impose an unjustified disproportionate and discriminatory burden on one group of individuals.

We note also that the very nature of the extremely sensitive work of civil actors, lawyers, human rights defenders in a democratic society is based on trust that information transmitted by victims and other interlocutors is without risk to them. It is clear that these individuals may be based abroad or, indeed, that it may be technically difficult to distinguish between national and foreign traffic. These concerns are obviously enhanced by the very broad and vague definitions used in the Counter-Terrorism act on which the secret surveillance is based.

**Conclusion**

In closing, I would like to refer to the most recent resolution of the Human Rights Council on the right to privacy in the digital age that states that the right to privacy “is one of the foundations of a democratic society”.[[6]](#footnote-6) The fragility of this right is such that even the possibility of its violation impacts the exercise of other fundamental freedoms enabled by it, and therefore affects key actors of a democratic society, and in, a democratic society. This is why the strict circumscription and control of the use of secret surveillance, including for counter-terrorism purposes, is essential.

I thank you for your attention.

1. Roman Zakharov v. Russia, para. 236. [↑](#footnote-ref-1)
2. Centrum för Rättvisa v. Sweden, para. 262. [↑](#footnote-ref-2)
3. A/HRC/39/29 [↑](#footnote-ref-3)
4. CCPR/C/POL/CO/7 para. 9. [↑](#footnote-ref-4)
5. Centrum för Rättvisa v. Sweden, para. 261. [↑](#footnote-ref-5)
6. A/HRC/RES/48/7/PP7 *Preamble.* [↑](#footnote-ref-6)