THE LEGALITY OF MASS ELECTRONIC SURVEILLANCE
IN INTERNATIONAL LAW

T. Ziniakova

In recent years the notion of mass electronic surveillance has received much attention in politics and international relations. Yet international law provides little guidance as to the normative regulation of surveillance practices. Such status quo poses a challenge before international law to define the phenomenon, analyze the legal implications it has for different actors and set out to develop principles and norms governing mass electronic surveillance.

First and foremost, it is essential to understand that surveillance exists in a number of forms. One of the most all-encompassing answers to the question «What types of surveillance are there?» was given in international legal doctrine [1, p. 9]:

Firstly, there is domestic surveillance targeted at the information stored within the surveilling State.

Secondly, there is foreign surveillance targeted at the information that either just passes through the surveilling State («transnational surveillance») or is stored entirely overseas («extraterritorial surveillance»).

Recognizing that domestic surveillance is a matter falling primarily within the national law of States, the research will only be concerned with foreign surveillance. Having analyzed existing doctrinal definitions [1, p. 9; 2, p. 5], the present article defines mass electronic surveillance as «clandestine or covert activities of a State consisting in collecting private information about another State’s officials or citizens using electronic means (including cyber-monitoring, telecommunications monitoring, satellites, or drones) and undertaken during peacetime».

Undoubtedly, there are numerous political reasons for States to engage in such activities, but the most plausible justification for conducting «mass cyber espionage» in international law remains the Lotus principle – embodied in an early decision of the Permanent Court of International Justice and stating that in the absence of a positive prohibitive rule, States are free to act at wide discretion [3, p. 19].

As it has famously been revealed by Edward Snowden in 2013, modern technologies (including those provided by most popular Internet services such as Microsoft, Google, Facebook and Skype) and progressive intelligence techniques are able to collect information in bulk about individuals worldwide. The unprecedented surveillance capabilities result in a conflict between the interests of national security and, firstly, the principle of non-intervention into domestic affairs of States, secondly, the principle of territorial integrity and, thirdly, the right to privacy. While the correlation of cyber espionage
practices with the first two principles does present academic interest and was touched upon in some international legal scholars’ works [4, p.32, 40–45; 5, p. 2], the present article will concentrate on the conflict between national security interests and the right to privacy.

Addressing the national security viewpoint, there is no need denying the widespread State practice of spying. That does not, nonetheless, indicate the presence of uniformed opinio juris which would make espionage a customary rule.

However, even accepting that spying in the best interest of national security is justified, it remains a question whether it would justify the practice with regard to a massive amount of individuals globally and not just the hostile States.

Addressing the right to privacy, one of the obvious sources to resort to when seeking privacy protection is the International Covenant on Civil and Political Rights («the ICCPR»). Under Article 17 of the Covenant States are to guarantee privacy to, as it follows from Article 2, paragraph 1 of the ICCPR, all individuals within their territory and subject to their jurisdiction [6]. Therefore Article 17 only covers domestic surveillance and the obligations of the surveilling States vis-à-vis its nationals.

In fact, in July 2013, Germany publicly expressed interest in amending the Covenant or concluding a protocol to it [7]. Germany’s goal was to clarify that the right to privacy contained in the ICCPR extends to electronic privacy, which may be different in its territorial scope.

Currently, as the concerns grow, steps are being made to have a meaningful discussion on the right to privacy in the digital age.

Both the General Assembly Resolution 68/167 of 18 December 2013 and the Report of the Office of the United Nations High Commissioner for Human Rights of 30 June 2014 recognize that the right to privacy must be protected online as well as offline [8, p.2; 9, p.4]. In the Report attempts are also made as to regulate the accountability of spying States for foreign surveillance based on the principle of the «effective control» [9, p.11].

Apart from the above-mentioned instruments of regulating the right to privacy in digital age, progress was also made in codifying, although unofficially, the guidelines for State conduct with regard to surveillance programs. International Principles on the Application of Human Rights to Communications Surveillance, developed by international NGOs, including «Privacy International» and «Electronic Frontier Foundation», are signed by 400 organizations and about 300 000 individuals [10].

Another important step was the introduction of the Special Rapporteur on the Right to Privacy in the Digital Age mandate in the Human Rights Council on 26 March, 2015.
The important conclusion drawn from the conducted research is that today’s challenge is not to eliminate mass electronic surveillance as such or to the maximum possible extent, but, given it exists and will continue to exist, – put it in an international legal framework, obliging the surveilling States to take account of the rights and interests of the most vulnerable groups involved.

There are a number of issues of professional interest within the mass electronic surveillance debate – from the evolutionary interpretation of the right to privacy to the matters of State Responsibility for the acts of foreign surveillance. Both academics and legislators are yet to thoroughly consider the correlation of national security concerns and human rights; as well as the correlation of national security concerns with the principles of international law, such as territorial integrity and non-intervention into domestic affairs of States. The current imbalance of those notions needs to be de-escalated by working on binding legal instruments and thus putting mass electronic surveillance into an international legal framework. All the mentioned issues are sure to be rapidly unfolding in front of the public eye in the nearest future, remaining the focal point of modern international law and requiring closest attention and comprehensive legal analysis.

Литература
5. Интернет-адрес: https://d1ovv0c9tw0h0c.cloudfront.net/files/2014/09/CDT-IL-surveillance.
7. Интернет-адрес: http://www.lawfareblog.com/2014/03/more-on-mass-surveillance.

ОСОБЕННОСТИ ПЕРЕВОДА СТРАДАТЕЛЬНОГО ЗАЛОГА В ТЕКСТАХ ПО СПЕЦИАЛЬНОСТИ «МЕЖДУНАРОДНЫЙ ТУРИЗМ»

А. И. Иватович

Действительный и страдательный залоги в английском языке совпадают со значением соответствующих залогов в русском языке. Глагол в действительном залоге показывает, что действие совершает лицо или