

CCBE Statement on the Pegasus scandal

1/02/2022

The Council of Bars and Law Societies of Europe (CCBE) represents the bars and law societies of 45 countries, and through them more than 1 million European lawyers. The CCBE places great emphasis on respect for human rights and the rule of law and is particularly concerned with the situation of human rights defenders around the world.

The CCBE notes that the newspaper consortium Forbidden Stories and Amnesty International revealed a leak of more than 50,000 phone numbers selected for surveillance purposes with Pegasus, a spyware sold by Israeli company NSO Group. The consortium revealed how this technology has been systematically abused for years to spy on lawyers, human rights defenders, journalists, academics, businesspeople, doctors, union leaders, diplomats, politicians, and several heads of states.

In particular, the leak of phone data suggests that lawyers and human rights defenders were selected by governments worldwide as possible candidates for invasive surveillance through their phones. The CCBE notes that lawyers from France, Hungary and the UK were targeted or selected as potential targets for surveillance. Rodney Dixon, a London-based lawyer, was selected for targeting in 2019. Forensic analysis of his device showed Pegasus-related activity but no successful infection. The phone of Joseph Breham, a French human rights lawyer was compromised several times in 2019¹. In Hungary, while the leaked data include the numbers of at least 10 lawyers², including János Bánáti, President of the Hungarian Bar association³.

Late December 2021, new revelations emerged about the use of Pegasus in Poland against a lawyer, Roman Giertych, who is known for representing politicians from the Polish opposition⁴. The President of the Polish Bar Council (*Naczelna Rada Adwokacka*) sent a letter to the Polish Prime Minister and other stakeholders asking whether the reports were true and, in the affirmative, on which legal basis Roman Giertych's phone was put under surveillance. In the letter, he explicitly emphasised the fact that such a surveillance raises suspicions that the activities violate professional secrecy, a principle that, in a democratic country, guarantee correct functioning of the State and justice⁵.

The CCBE would like to express its serious concern over the so-called "Pegasus scandal" and the surveillance or potential surveillance of lawyers. In this regard, the CCBE has repeatedly stressed the importance of professional secrecy and legal professional privilege. The European Court of Justice itself expressly stated "*that confidentiality serves the requirements, the importance of which is recognized in all of the member states, that any person must be able, without constraint, to consult a lawyer whose profession entails the giving of independent legal advice to all those in need of it*", and added that *the principle of "the protection against disclosure afforded to written communications between lawyer and client is based principally on a recognition of the very nature of the legal*

¹ <https://www.theguardian.com/news/2021/jul/19/spyware-leak-suggests-lawyers-and-activists-at-risk-across-globe>

² <https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests>

³ <https://telex.hu/direkt36/2021/07/20/pegasus-nso-surveillance-hungary-lawyers-bar-association-janos-banati>

⁴ <https://www.politico.eu/article/polish-spyware-scandal-stokes-up-tensions-with-eu/>

⁵ <https://twn24.pl/najnowsze/y7xpe3-Pismo-prezesa-Naczelnej-Rady-Adwokackiej-do-premiera-Mateusza-Morawieckiego/file-20211221-premier-32714.pdf>

profession, inasmuch as it contributes towards the maintenance of the rule of law and that the rights of the defence must be respected”⁶.

This core value of the legal profession is under attack by the use of sophisticated technical capabilities by private or public entities, such as state bodies. Nowadays, lawyers have no choice but to use modern technology when communicating with clients, courts, lawyer colleagues and others. Yet it appears that such technology is not safe to use, no matter how prudently the lawyer uses it. The CCBE underlines that the erosion of the confidentiality of lawyer-client communications also erodes the trust of a citizen in the administration of justice and the rule of law.

Therefore, the CCBE calls upon national and European authorities, through EU institutions and the Council of Europe, to take steps to protect and enhance the confidentiality of lawyer-client communications when modern technology is used. Such steps should include both legal and technical work by, for example, clarifying the responsibility of any publisher making available such tools to third parties that is capable of illegal use; prohibiting the publication of such tools worldwide outside national security services; ensuring that such tools are only accessible to those national security services for whose acts the publishing state takes full responsibility; or by issuing mandates for standardisation work to make such end user devices safer to use.

Furthermore, it should be ensured that material protected by professional secrecy and legal professional privilege is out of the scope of surveillance operations through instruments of international law, such a European Convention on the legal profession.

Finally, the CCBE invites national and European authorities to take consideration of its recommendations on the protection of fundamental rights in the context of ‘national security’⁷ as well as on the protection of client confidentiality within the context of surveillance activities⁸.

⁶ ECJ, 1982, AM&S (155/79).

⁷ CCBE recommendations on the protection of fundamental rights in the context of ‘national security’, 2019

⁸ CCBE recommendations on the protection of client confidentiality within the context of surveillance activities, 2016