Jesper Lund
IT-Pol Denmark and EDRi
jesper@itpol.dk

Spyware and e-privacy, PEGA Committee hearing, 26 October 2022

Dear members of the PEGA Committee

Thank you for inviting me to speak about spyware and e-privacy.

European Digital Rights is a network of civil society organisations that work to defend and advance digital rights across Europe. I am chairman of the Danish member IT-Pol, and representing EDRi today.

Outline

In my intervention, I will first consider whether the existing ePrivacy framework offers legal protection against spyware. Secondly, I will suggest possible ways forward for improving the legal protection against spyware by other instruments of EU law.

ePrivacy Directive

The main instrument to protect confidentiality of communications in EU law is the ePrivacy Directive (ePD). We are still waiting for the ePrivacy Regulation to be adopted, even though the proposal was presented in January 2017, almost six years ago.

The ePrivacy Directive applies to providers of publicly available electronic communications services.

The Directive protects confidentiality of communications by requiring service providers to delete or anonymise communications content and metadata after transmission of the communication. This is the main rule with some limited exceptions.

CJEU case law

The CJEU has interpreted the ePD in a number of cases about national data retention laws and access to retained data by public authorities.

A common aspect of the cases decided so far is that the national laws impose obligations on private service providers to either retain data or disclose data to public authorities.

Since these measures require processing by service providers, they constitute restrictions of the rights and obligations provided for by the ePD. The restrictions must satisfy the conditions of Article 15(1) of the ePD interpreted in light of the Charter.

This has the effect of bringing national laws within the scope of the ePD and hence EU law, even if the purpose is safeguarding national security, which is noteworthy. Member States cannot circumvent the protection under EU law by invoking broad definitions of national security.

However, the critical connection to the ePD is the processing obligations for service providers.

In paragraph 103 of the La Quadrature du Net ruling from October 2020, the CJEU states that if Member States derogate from the protection of confidentiality of communications without imposing obligations on service providers, the protection of personal data is not covered by the ePD. It is only covered by national law, possibly subject to the application of the LED.

Applicability of the ePD to spyware

I will now turn to the question of whether the ePD and the associated CJEU case law is applicable to national laws on deployment of spyware by either law enforcement or intelligence services.

Spyware such as Pegasus from NSO Group is deployed by exploiting software vulnerabilities on the devices (e.g. smartphones) of the persons targeted to this surveillance measure. To put it bluntly, by hacking their devices.

The interference with the device is either done directly by state authorities or with the assistance a private spyware vendor such as NSO. In terms of the ePD, the spyware vendors are clearly not providers of electronic communications services.

Since the deployment of spyware is done entirely without any processing by a provider covered by the ePD, the case law of the CJEU would suggest **that the ePD does not apply** to the processing of personal data.

However, there are other factual differences between the deployment of spyware and the cases considered by the CJEU so far. This creates an alternative connection to the ePD which does not require processing by providers of electronic communications services.

Article 5(3) of the ePD protects the user's terminal equipment against interference, which also covers smartphone devices. Often referred to as the "cookie law", the storing of information or gaining access to already stored information in the user's terminal equipment is only allowed with the consent of the user. The only exception to consent is if the processing is strictly necessary for an information society service explicitly requested by the user.

Unlike the other provisions of the ePD, the scope of Article 5(3) is not limited to providers of electronic communications services.

Since the conditions in Article 5(3) are clearly not satisfied for the deployment of spyware, it could be argued that the deployment constitutes a restriction of the right to protection of terminal equipment afforded by the ePD, and that this restriction is subject to Article 15(1). This would put national laws on spyware within the scope of the ePD similar to national data retention laws.

A case is pending before the CJEU which could perhaps resolve the legal uncertainty about the applicability of the ePD to spyware. The case number C-548/21 from Austria is about extracting information from a mobile device with physical access, so not entirely the same as remote deployment of spyware. But the case is similar in terms of the possible interference with the user's terminal equipment and in particular the lack of processing obligations for service providers.

Other instruments of EU law

Deployment of spyware could, of course, be regulated by EU law in other ways than the ePD.

The first to consider here is the hopefully future ePrivacy Regulation. As the text currently stands with Parliament and Council positions in trilogue negotiations, the ePrivacy Regulation will have largely the same scope as the current Directive. This also means the same limitations with regard to protection against spyware.

The recent proposal for the European Media Freedom Act takes a much more direct approach to regulating the deployment of spyware by Member States. Article 4 of the proposal creates rights for media service providers which include protection against deployment of spyware, though with some exceptions.

These exceptions are rather broad and leave so much discretion to Member States that the protection could easily be undermined. However, this part of the provision could, and should, be strengthened.

A similar and preferably stronger protection of the confidentiality of communications against deployment of spyware could be extended to all individuals in the EU in a future legislative proposal.

Importance of EU law protection

I will conclude my intervention by highlighting two reasons for importance of having effective protection against spyware in EU law.

The first reason is the abuses of Pegasus and other spyware uncovered by the investigations of civil society organisations, journalists and the work of this committee. National laws of Member States do not provide adequate protection and safeguards. EU law should address this and uphold the protection of fundamental rights.

The second reason is to counterbalance the increased information exchange between Member States, in part facilitated by EU law and EU agencies. The recently amended Europol Regulation allows Europol to receive and analyse large datasets from Member States. Large datasets can include electronic communications data obtained from bulk collection operations with spyware. The EncroChat investigation is an example of that.

Unlike traditional wiretapping of telephone services, spyware can be easily deployed across national borders. Protections against spyware in national law can therefore be undermined if other Member States can deploy spyware, especially in an indiscriminate manner, and then share the information obtained through Europol or other channels. To prevent a race to the bottom for fundamental rights, EU law should set minimum legal standards for the deployment of spyware by Member States.

The EDRi position paper on encryption, published last Friday on Encryption Day, offers concrete proposals on how State hacking, as we call it, can be regulated.

This concludes my intervention. I thank you for your attention and look forward to your questions.