Constitutional complaint regarding the police's handling of security vulnerabilities in IT systems is inadmissible

Press Release No. 62/2021 of 21 July 2021

Order of 8 June 2021
1 BvR 2771/18

IT security vulnerabilities

In an order published today, the First Senate of the Federal Constitutional Court dismissed a constitutional complaint regarding the state's exploitation of IT security vulnerabilities that the developers of the software or hardware are not yet aware of (so-called zero-day vulnerabilities). The constitutional complaint is inadmissible because the alleged breach of the duty of protection against unauthorised third-party access to IT systems – a duty arising from fundamental rights – has not been sufficiently substantiated and the requirements stemming from the principle of subsidiarity in a broader sense have not been met.

Facts of the case:

§ 54 of the Baden-Württemberg Police Act in the version of 6 October 2020 (*Polizeigesetz Baden-Württemberg* – PolG BW) allows for the covert surveillance of the contents of telecommunications for the purpose of preventive police work in order to protect certain weighty legal interests. Pursuant to § 54(2) PolG BW, which is the provision challenged by the complainants in these proceedings, surveillance may be carried out through interference with IT systems if technical measures are in place to ensure that telecommunications are only intercepted and recorded in real time and if the interference is necessary to intercept and record telecommunications, particularly in unencrypted form. Performing this kind of source telecommunications surveillance under § 54(2) PolG BW involves infiltrating the targeted system with surveillance software. This can be done in various ways. The constitutional complaint solely concerns infiltration by way of exploiting zero-day vulnerabilities in the hardware or software of the targeted system.

The complainants essentially assert that, by enacting the authorisation laid down in § 54(2) PolG BW, the *Land* Baden-Württemberg violated the right to protection of the confidentiality and integrity of information technology systems – as guaranteed by fundamental rights – because under that provision, the authorities have no interest in notifying developers of any vulnerabilities that come to their attention since they can exploit these vulnerabilities to infiltrate IT systems for the purpose of source telecommunications surveillance, which is permitted under § 54(2) PolG BW. Yet if the developers are not notified, these vulnerabilities and the associated dangers – in particular the danger of third-party attacks on IT systems – will continue to exist. The complainants contend that Baden-Württemberg failed to create the absolutely necessary accompanying provisions with regard to vulnerability management – provisions that would have to prohibit the exploitation of security vulnerabilities unknown to the developer of the respective system. They argue that even if the exploitation of zero-day vulnerabilities were not deemed inherently incompatible with the state's duty of protection, administrative procedures must at least be established for evaluating IT security vulnerabilities on a case-by-case basis.

Key considerations of the Senate:

The constitutional complaint is inadmissible.

I. The complainants have not sufficiently demonstrated their standing to lodge a constitutional complaint. It is true that the state has a duty of protection arising from fundamental rights in this case; the privacy of telecommunications is affected, as is the protection of the confidentiality and integrity of information technology systems, which is guaranteed by fundamental rights. However, the complainants have not sufficiently substantiated a breach of the duty of protection arising from these fundamental rights.

1. The state has a duty of protection in this case. In order to protect fundamental rights, the state bears a responsibility for the security of IT systems. In the circumstances under review in the present case where the authorities are aware of a vulnerability that is unknown to the developer, the state has a specific duty of protection arising from fundamental rights.

The state must contribute towards protecting the users of IT systems against third-party attacks on those systems.

a) In this case, the state's duty of protection follows from the fact that affected persons are unable to protect themselves even though a state authority is aware of the security vulnerability; this duty also follows from the major risk or damage that such IT security vulnerabilities can potentially cause. On the one hand, this puts informational self-determination at risk given that extensive knowledge of personal matters can be obtained by gaining access to a user's data. On the other hand, security vulnerabilities have the potential to cause damage far greater than the disclosure of personal information given that third parties who infiltrate and manipulate IT systems via security vulnerabilities are capable of disrupting a large variety of processes – industrial and commercial processes, for example – to the detriment of affected persons. The risk of being infiltrated by third parties is also associated with the particular danger of being blackmailed.

b) In the present case, the duty of protection encompasses the obligation for the legislator to set out how the police are to handle such IT security vulnerabilities. Under constitutional law, it is not inherently impermissible from the outset for source surveillance to be performed by exploiting unknown security vulnerabilities, although stricter requirements for the justification of such surveillance apply due to the dangers posed to the security of IT systems. Furthermore, fundamental rights do not give rise to a claim that authorities must notify developers about any IT security vulnerabilities immediately and in all circumstances. However, the duty of protection does necessitate a legal framework that governs how – in a manner compatible with fundamental rights – an authority is to resolve the conflicting aims of protecting IT systems against third-party attacks that exploit unknown IT security vulnerabilities on the one hand, and on the other hand keeping such vulnerabilities open so that source surveillance can be carried out for the purpose of maintaining public security.

2. The complainants have not sufficiently demonstrated that this duty of protection arising from fundamental rights might have been breached.

a) It is for the legislator to establish and implement a protection strategy. The legislator generally has a margin of appreciation, assessment and manoeuvre in this respect. This means that constitutional complaints asserting that the legislator has breached its duty of protection must satisfy a special burden of substantiation. Such constitutional complaints must address the entire regulatory context of a legal provision. This includes at least outlining the relevant provisions of the challenged regulatory framework and stating reasons as to why they provide insufficient protection under constitutional law.

b) The constitutional complaint does not satisfy these substantiation requirements since the complainants have not outlined the various legal provisions concerning the protection of IT systems that might be significant in the present context, nor have they put forward specific reasons why these provisions fall considerably short of the aim of protection, including when viewed as a whole.

The legal authorisation itself encompasses various safeguards that the legislator actually included with the specific aim of "protecting data security also with regard to third-party interferences". The complainants would have needed to address § 54(3) second sentence PolG BW, which states that the method employed must be protected from unauthorised use. The conflicting aims could also be addressed in the context of a data protection impact assessment pursuant to § 80 PolG BW but the complainants did not deal with the open questions regarding the interpretation of the constituent elements of the provision. Moreover, they did not sufficiently address the extent to which the Baden-Württemberg Act on Improving Cyber Security – which entered into force on 17 February 2021 – contains safeguards. And finally, they do not mention the agreement that significant IT security incidents must be reported – an agreement reached in the context of the State Treaty on the Establishment of the IT Planning Council and on the Principles of Cooperation Underlying the Use of Information Technology in the Administrations of the Federation and the *Länder*.

II. Furthermore, the constitutional complaint fails to satisfy the requirements arising from the principle of subsidiarity in a broader sense.

These requirements mean that in addition to the remedies formally available for achieving the immediate aim of legal action, all the available procedural options must be exhausted in order to remedy a violation of fundamental rights. This serves the purpose of ensuring that in a first step, the ordinary (non-constitutional) courts – which are primarily responsible for the interpretation and application of ordinary law – deal comprehensively with the points of fact and law while also taking into account the standards arising from constitutional law, thereby preventing the Federal Constitutional Court from having to take far-reaching decisions on an uncertain factual and legal basis. In the case at hand, complex questions arise concerning the interpretation of ordinary law. Whether, under the law as it currently stands, authorities are already obliged to carry out a balancing that gives effect to the duty of protection arising from fundamental rights before deciding to notify the developer about a zero-day vulnerability that has come to their attention depends on how various provisions of police law, data protection law, cyber security law and IT security law are interpreted. These provisions are largely part of more recent ordinary law and their significance has not yet been precisely delineated through court decisions, other applications of the law or legal scholarship. This makes it necessary to seek legal recourse before the ordinary courts by filing an action for a declaratory judgment or an action for a pre-emptive injunction – steps which would be reasonable (*zumutbar*) for the complainants in the present case.