Police Act and Constitution Protection Act **Hesse**

8-10 minutes

The GFF, jointly with the Humanist Union, the Data Protectionists Rhine Main and the Forum Computer Scientists for Peace and Social Responsibility, has filed a constitutional complaint against the Hessian Police Act and Constitutional Protection Act. The complaint is directed against an amendment to the law that massively expands the surveillance powers of the police and the Office for the Protection of the Constitution. In Hesse, the authorities are now allowed to use so-called state Trojans. The Hessendata software is used to analyze personal data centrally and automatically. This automated data evaluation was the subject of a hearing before the Federal Constitutional Court in December 2022. In February 2023, the Federal Constitutional Court upheld our complaint in large parts and declared the power of automated data evaluation unconstitutional.

In 2018, Hesse followed the nationwide trend toward stricter police laws that often violate fundamental rights. The amendment to the law of July 4, 2018, gives the police partly expanded and partly new options for monitoring information technology systems. For example, the legal basis for monitoring ongoing communications (so-called source TKÜ) contained in the Hessian Security and Order Act (HSOG) was expanded, and legal bases for online searches and the use of Big Data analysis software were created.

HEARING BEFORE THE FEDERAL CONSTITUTIONAL COURT: HESSENDATA ANALYSIS SOFTWARE ALLOWS COMPREHENSIVE SURVEILLANCE OF INDIVIDUALS

The focus of the oral hearing at the Federal Constitutional Court in December was on automated data analysis with the help of the analysis software Hessendata by the US company Palantir. Large amounts of personal data flow into the data analysis: data from police databases, from telephone surveillance, read-out mobile phone data but also external data, for example from social media or data requested by other authorities.

With the complex data analysis, the police want to shed light on networks and structures in order to prevent future crimes. Anyone who becomes the focus of a data analysis quickly becomes a virtually transparent citizen. Numerous other people are also affected by the analysis as "by-catch": The same address or the same football club can be enough for the software to draw connecting lines.

JUDGES ASK CRITICAL QUESTIONS

The legal basis for the use of the software is extremely vague and leaves many questions unanswered - this also became clear in the trial, in which both the Hamburg and the Hesse laws were discussed: Is - as according to the respective government representatives - the Automated Data Analysis only the continuation of classical police work with "more power"? Or does the possibility of pulling together huge pools of data, generating connections and

patterns, justify a whole new quality of intervention that also needs correspondingly strict limits? The Hessian interior authorities did not tire of affirming that no artificial intelligence was being used. The subject of the proceedings, however, were the regulations and they are - as has been formulated again and again today - "open to technology". What is not yet, can therefore - according to the law - still become at any time.

The many detailed questions from the court showed that the judges were also critical of the vague norms on automated data evaluation. In particular, the question was raised at many points whether compliance with the legal limits is technically feasible at all. For example, the court probed the keyword "purpose limitation": Once collected, data may not be used for another purpose without further ado. At present, however, the origin of the data is not marked at all - how is compliance with the purpose limitation supposed to work when the data is further processed?

The judges also dealt extensively with the wording in the Hessian law according to which automated data evaluation is only permitted in "justified individual cases". They asked exactly how compliance would be monitored and made it clear that they saw too few indications in the law as to which limiting criteria should be used here.

The severity of the encroachment on fundamental rights requires a concrete danger. However, Hessendata may already be used in advance of a concrete danger for the preventive prevention of criminal offences. With our constitutional complaint, we want to subject this practice to constitutional control.

HESSIAN TROJAN INTRODUCED

These changes endanger the IT security of all citizens. TKÜ and online searches require the installation of government spying software on a device. IT security vulnerabilities are exploited for this purpose. This sets the wrong incentives for the police: Instead of reporting security gaps to the manufacturers, the police may keep them secret and exploit them for surveillance measures. However, the same security gaps can then be used by cybercriminals and foreign intelligence agencies for cyberattacks. The so-called Hessian Trojan thus violates the fundamental right of all citizens to the guarantee of confidentiality and integrity of information technology systems, or in short IT fundamental right.

FEDERAL CONSTITUTIONAL COURT LIMITS AUTOMATED DATA MINING BY THE POLICE

In February 2023, the judges in Karlsruhe made it clear in a landmark ruling that the police may, in principle, use software to create information and cross-references to individuals at the push of a button in order to prevent criminal offences (data mining). However, the law must clearly stipulate the conditions under which this is permissible. Otherwise, the regulations violate the right to control one's own data. Among other things, we had attacked the fact that the legal basis in Hesse leaves it completely unclear from which sources, with which amount of data and for which purpose the police may use the power of data mining. Our constitutional complaint has significantly reduced the risk of innocent citizens being targeted by the police. The ruling has a nationwide impact: many other federal states and the federal government are working towards being able to use comparable technical possibilities - or are already doing so, such as North Rhine-Westphalia.

NEW POWERS FOR THE HESSIAN CONSTITUTIONAL PROTECTION SERVICE

The amendment also comprehensively revised the Hessian Law on the Protection of the Constitution (HSVG). The requirements for surveillance measures are far too low: The Office for the Protection of the Constitution may, for example, use undercover investigators and informers, as well as make requests for information to transportation companies, if this is necessary for the fulfillment of its tasks and without there having to be an actual threat situation. Once data has been collected, the Office for the Protection of the Constitution can forward it to other public agencies and foreign governments almost without any conditions. Data subjects themselves have only very limited rights to know what data has been collected about them.

GOVERNMENT INTERFERENCE WITH CIVIL LIBERTIES

In Hesse, too, the expansion of police and constitutional protection powers is accompanied by serious encroachments on civil liberties. For an uncertain gain in security, the state government is accepting serious encroachments on general personal rights and a massive threat to IT systems worldwide.

The constitutional complaint was brought by seven complainants. In addition to the HU regional chairman Franz Josef Hanke, they include the lawyer Seda Basay-Yildiz, Klaus Landefeld as a board member of the Association of the Internet Industry eco and DE-CIX Supervisory Board, as well as Silvia Gingold, a retired teacher and daughter of the Jewish resistance fighter Peter Gingold, who has been under observation by the Office for the Protection of the Constitution since her youth due to her anti-fascist commitment.