New laws legalize police state operations in Germany

Part one: The new Verfassungsschutz Law and the new Federal Intelligence Agency Law

Wolfgang Weber
2 July 2021

Germany's ruling Grand Coalition of the Christian Democratic Union, Christian Social Union and Social Democratic Party has used the final parliamentary sessions of the current legislative period to massively expand the powers of the country's police and intelligence agencies. Largely unnoticed by the public, the Bundestag has passed a total of nine related laws and amendments.

The new government to be formed after the federal election due this autumn will have at its disposal a technically highly equipped surveillance apparatus, with powers the likes of which have not been seen in Germany since the end of the Nazi regime. The state security apparatus (nicknamed Stasi) of the former East Germany, with its network of neighbourhood snoopers and its note box system, appears amateur in comparison.

Taken together, the legislative changes passed by the Bundestag since November 2020, and especially in the last four weeks, represent the biggest legislative complex passed since the reunification of Germany in 1990. Its main features are as follows:

Almost complete abolition of the separation of the police and secret services introduced after World War II in response to the experience of Hitler's Secret State Police (Gestapo).

The Federal Police (Bundespolizei) now has powers equivalent to those of a secret service, while the secret services can undertake police tasks. Both agencies will in future work hand in hand.

* The Federal Police will be able to massively restrict the freedom of citizens and refugees via bans on staying, detention pending deportation and similar measures, without requiring judicial authorisation.

* The powers of the police and secret services to tap into computer systems, mobile devices and other electronic systems in order to gather and/or manipulate data on a massive scale are being legalized.

* Authorisation is being granted for the secret services and Federal Police to carry out cyber-attacks and other observation and persecution measures merely on the basis of a targeted person's opinions, without any evidence of criminal activities.

* New powers are being authorized to comprehensively deploy automated monitoring and censorship of the internet with the help of upload filters.

* Seamless centralised collection and storage of personal and biometric data, made accessible to all state authorities, is being legalized.

Repression of the population, rather than its security, is the single purpose of the new laws. The entire state apparatus is being armed to suppress growing popular resistance to the devastating consequences of the coronavirus pandemic, attacks on jobs and social rights, militarism and war, and the threat from neo-Nazis and fascists.

The new Protection of the Constitution Law

The "Protection of the Constitution Law," passed by the Bundestag on 10 June 2021, legalises the extensive use of so-called "State Trojans" by the Bundesamt für Verfassungsschutz (Federal Office for the Protection of the Constitution—Germany's domestic secret service), the 16 Landesämter für Verfassungsschutz (State Offices for the Protection of the Constitution), the Federal Intelligence Service (foreign intelligence agency—BND) and the Military Counter-Intelligence Service (MAD). All of these 19 secret services can now systematically spy on people at home and abroad. The law sets virtually no limits on the data that may be collected and the reasons for observation.

A State Trojan is malware placed by an intelligence agent on the smart phone, laptop, PC or server of a person or organisation to be observed during a clandestine invasion of his or her home, or remotely via the internet. The monitoring of an ongoing communication takes place on the targeted person's device before the conversation, chat message or SMS is encrypted.

The operation is also referred to as telecommunication source tapping. The use of a State Trojan with the aim of transmitting stored data such as documents, image recordings and video recordings to the intelligence service is known as an online search.

In addition, State Trojans can manipulate data and programmes on other people's computers, mobile phones and IT systems, with far-reaching, possibly fatal consequences for the persons concerned. A vehicle's electronic control and braking systems can, for example, be manipulated to cause an accident.

Telecommunication source tapping and online searches were previously legally permitted only by the Federal Criminal Police (BKA), in the context of police investigations ordered by a judge into serious crimes. Now, all secret services have the power to conduct such operations.

According to the wording of the new law, the secret services are not permitted to carry out online searches. They are, however, allowed to extract data stored on a targeted device after a Trojan has been activated. In practice, nothing can prevent agents from collecting data stored much longer. Technically, a telecommunication source tapping operation is capable of carrying out a complete online search at the same time.

Several experts have sharply criticised the new Protection of the Constitution Law, declaring it to be unconstitutional. Dr. Matthias Bäcker, professor of public law and information law at the University of Mainz, stated in an expert opinion that all malware operations not strictly limited to an ongoing communication are online searches. If they are now carried out in the name of telecommunication source tapping, bypassing all legal hurdles, this will constitute a violation of the basic right to the integrity and confidentiality of information technology systems, he said. [1]

The Mainz professor also criticised the fact that the latitude for hacking and spying attacks has been considerably expanded. The law allows "telecommunication surveillance in part even in the case of the planning of comparatively minor offences." As examples, Bäcker mentions "the dissemination of propaganda material of anti-constitutional organisations, violations of a ban on associations and membership of a secret association of foreigners." [2]

In addition, the new law has expanded the concept of "anti-constitutional aspirations" from organisations to individuals, whereby the "target of their behaviour" is sufficient justification to start intelligence agency observations. Bäcker warns that the law "virtually invites a practice of observation based on (presumed) personal characteristics or the social ties of the persons concerned, instead of on actions objectively relevant to the intelligence agency." [3]

In other words, persons are observed and prosecuted not because of concrete acts, but because of their opinions.

This principle of Gesinnungsjustiz (judgement based on opinions) was the basis of the legal system of the Nazis and is also the basis for the observation of the Sozialistische Gleichheitspartei (Socialist Equality Party—SGP) by the Verfassungsschutz. When the Verfassungsschutz first included the SGP as a "left-wing extremist party" in its annual report of 2017, it justified its action by stating that the SGP defended a socialist programme, criticised capitalism and politically criticised apologists for capitalism—in particular the SPD, the Left Party, the Greens and the trade unions.

When the SGP subsequently filed a complaint against this judgement, lawyers for the Verfassungsschutz justified the persecution of the SGP not on the basis of unlawful activities, but rather on the basis of the party's analysis of society, its Marxist stance on history, its political analyses and its socialist objective. The Verfassungsschutz lawyers stated that "arguing for a democratic, egalitarian, socialist society" contradicted "the central values of Germany's Basic Law." [4]

The SGP warned at the time: "With its attack on the SGP, this criminal government agency wants to set a precedent for a new kind of legal prosecution of thought crimes that would provide the basis for the prosecution of anyone who criticises the current reactionary social and political situation… If the right-wing conspiracy in the state apparatus is not stopped and the SGP is not defended, the dam will be broken for even more far-reaching measures." [5]

This assessment has now been confirmed. The new Protection of the Constitution Law legalises hitherto unprecedented measures targeting broad sections of the population and all kinds of organisations and parties assessed to be undesirable by the intelligence agencies and the German government.

In order to carry out this surveillance technically, the law obliges companies active in the aviation, financial services, telecommunications and telemedia sectors to pass on the personal data of citizens under surveillance and provide technical assistance for the insertion of State Trojans for online searches and the transmission of the resulting data streams. Internet providers such as Telekom and Vodafon, but also Google, Facebook and banks, will be turned into accomplices of the secret services.

Only a few target groups, such as priests and lawyers, are exempt from secret service cyber-attacks. Journalists—despite protests from journalists' associations—are explicitly not among them. The freedom of the press and the digital protection of its sources have been gutted.

The law also provides for networking and data exchange between all of the various secret services, Federal Police, Federal Criminal Police and other state authorities such as the country's immigration authorities and the Federal Employment Agency.

The new Federal Intelligence Service Law

The Federal Intelligence Service Law of 25 March 2021 legalises the tapping of huge databases and data streams to monitor the communications of millions of people and search their computers, mobile phones and servers for data, photos and videos by the BND, the foreign intelligence service.

This same law was supposed to fulfil legal requirements to restrict and control the activities of the BND, as stipulated by the German Constitutional Court in May 2020. The court declared that the previous law of 2016, which legalised the mass surveillance uncovered by American whistleblower Edward Snowden, to be unconstitutional.

The court, however, did not object to mass surveillance per se, but merely insisted on compliance with a few formalities in its ordering, documenting and monitoring. It thereby provided a flimsy democratic fig leaf for mass surveillance.

But even with these formalities, the changes in the new BND law compared to the old one are minimal or simply *farcical*. For example, the quantitative limitation of interceptions demanded by the Federal Constitutional Court is implemented in such a way as to cover not more than "30 percent of the transmission capacities of all globally existing telecommunications networks!"

What looks like a limitation is, in reality, a licence for unlimited spying. The BND, even if it continues to greatly expand its technical capabilities, will never be able to collate the enormous amount of data associated with this "limit," according to Klaus Langenfeld, a man who should know. He is the operator of the world's largest Internet node DE-CIX, near Frankfurt am Main, which at peak times records a data flow of more than 10 terabits, or 10 trillion bits per second. [6]

The new law also significantly expands the power to intercept data and spy on people. The BND is allowed to hack communication providers such as Google, Apple, Facebook, Amazon, Microsoft and Vodafone, as well as the IT systems of foreign companies and authorities, "even without their knowledge" and "without concrete cause." These shady and criminal operations are called "strategic telecommunications reconnaissance" in the jargon of the ministerial authors.

Significantly, not only foreign but also German citizens, companies and IT systems may be targeted by the BND. Formally, the law prohibited the surveillance and interception of the "individual communications of natural persons," even though no one can control compliance with this prohibition. The use, however, of a smart phone, computer or even a telephone is considered communication with machines. In these cases, the BND is allowed almost unrestricted access to stored data and current traffic and content data.

For such operations, the BND is explicitly allowed to cooperate and exchange data with foreign intelligence services such as the National Security Agency (NSA) and thereby use huge secret data storage centres such as the one in Utah. As Edward Snowden has revealed, the BND has been carrying out such operations for years, without any legal basis. Now the laws have been adapted to this practice!

As already mentioned, the BND is also allowed to use State Trojans for the mass extraction of data from foreign IT systems and devices.

The range of "dangerous topics" which the BND is authorized to spy upon has also been considerably expanded. In addition to the previous topics—international terrorism, the transfer of nuclear weapons material and illegal smuggling—"crisis developments abroad," "protection of critical infrastructures" and "cases of intellectual property theft" or copyright infringement have been added.

The latter marks the first time a secret service has been authorised by law to intervene in private legal disputes. German companies are to be strengthened against foreign competitors. Chinese companies in particular have long been accused of copying products and programmes, although no evidence of such activities has ever been provided.

Now, with the help of the BND, it is hoped that such evidence can be found or fabricated as a pretext for more aggressive action against China.

US companies are also likely to appear soon as targets on the monitors of the BND. The growing tensions between Germany and the US are part of the background to the BND's increased powers.

Particularly dangerous is the BND's new task of monitoring, spying on, sabotaging or manipulating oppositional tendencies, organisations and individuals at home and abroad under the catchword "international extremism." These operations are based on the same principle of a thought police utilised by the Verfassungsschutz.

The BND was founded in 1956 by Reinhard Gehlen, who was responsible for military espionage against the Soviet Union under Hitler. Its staff consisted mainly of former agents of the Nazi military espionage apparatus, Gestapo and SS. Gehlen even collaborated with war criminals and Holocaust mass murderers such as Klaus Barbie, who had gone into hiding in Bolivia. [7]

Germany's Grand Coalition has now turned this organisation, steeped in its Nazi past, into a kind of super-intelligence agency for use against foreign countries and against its own people. The BND reports directly to the German Chancellery and has over 6,500 official employees, as well as enormous financial resources—this year alone over half a billion euros. For the past two years, it has resided in Europe's largest new building complex in the centre of Berlin.

Part two of this article will deal with other new police state legislation and provide a political assessment.

**

Notes

[1] Dr. Matthias Bäcker, statement on the draft for the Adoption of the Law on the Protection of the Constitution, Bundestag papers 19/24785; p. 13

[2] ibid., pp. 14-15

[3] ibid, pp. 4-6

[4] See: "Stop the right-wing conspiracy! Defend the SGP against the Verfassungsschutz secret service!" https://www.wsws.org/en/articles/2019/07/26/sgps-j26.html

[5] ibid.

[6] See: https://netzpolitik.org/2021/bnd-gesetz-bundesnachrichtendienst-erhaelt-so-viele-ueberwachungsbefugnisse-wie-noch-nie/

[7] See: "How former Nazi official Reinhard Gehlen erected a state within a state in post-war Germany" https://www.wsws.org/en/articles/2017/12/27/germ-d27.html