VIENNA / 12th of September 2024

State Trojan 2024

Draft of a federal law with which the State Protection and Intelligence Service Act (Staatsschutz- und Nachrichtendienstgesetz or „SNG“) is amended

For epicenter.works
Sebastian Kneidinger
Tanja Fachathaler
Thomas Lohninger

EPICENTER.WORKS
for digital rights

FOREWORD AND EXECUTIVE SUMMARY

We are grateful for the opportunity to submit the following statement as part of this bill's review process.[1] Since 2016, epicenter.works has extensively dealt with the various demands and legislative attempts to legalize the use of a **„state trojan“ (a software that would enable the monitoring of encrypted messages)**.[2] In recent years, we have explained in numerous statements why this measure **does not guarantee the alleged goal of increasing national security**, but rather **jeopardizes IT security** and **disproportionately interferes with the fundamental rights of** all people residing in Austria.

In its ruling in December 2019, the Austrian Constitutional Court clarified the extent to which a state trojan interferes with fundamental rights. Of particular importance was the court's finding that the confidential use of computer systems and electronic communications services is a central element of the right to respect for private life in accordance with Art 8 ECHR. The increasing relevance of digital technologies makes them a crucial means of personal development and private life. Data on the use of such systems offers insights into the most intimate areas of life and allows conclusions to be drawn about users' thoughts, preferences and beliefs.[3] The court also recognized, that the use of a state trojan often also incidentally collects data on numerous uninvolved persons. Thus, the use of a state trojan is considered a serious invasion of privacy that is only permissible under strict conditions. The draft in question from our point of view does not meet these high requirements.

A look at international case law illustrates the **central importance of encryption** for the protection of privacy and against state surveillance. The attempt by the Russian secret service FSB to demand a "backdoor" from Telegram to decrypt messages was found to be a clear violation of fundamental rights by the European Court of Human Rights as recently as February of this year.[4] **The ECtHR emphasized that encryption not only protects privacy, but also prevents criminals from accessing sensitive data.**

We see the creation and preservation of "backdoors," such as those required for the use of a state trojan, as a threat to the security of all users. These "backdoors" make the entire flow of communications vulnerable to cybercrime, data leaks and unauthorized access. Any attempt to circumvent encryption undermines trust in digital communication platforms and jeopardizes both privacy and freedom of expression. Therefore, the protection of encryption in a democratic society must not be weakened, especially not to achieve short-term surveillance goals. **Instead, the state should fulfill its duty to protect**[5] and ensure appropriate IT security.

Although the present draft law attempts to reduce the extent fundamental rights are infringed by limiting the use of a state trojan to surveillance of communications and providing stronger legal protections than its predecessor, it still falls short of the requirements of fundamental rights and technical realities in both respects:

The restriction of the state trojan to merely access to messages is **a legal fiction** that fails in the face of the technical reality. A state trojan inherently requires full administrative access to a cell phone. Due to

[1] 350/ME XXVII. GP , Link: https://www.parlament.gv.at/gegenstand/XXVII/ME/350

[2] Further information on our activities can be found here: https://epicenter.works/en/thema/state-trojan

[3] Cf "*Vehicle license plate recognition and "federal Trojan" unconstitutional*" Media release of the Constitutional Court. 11.12.2019 , Link: https://www.vfgh.gv.at/medien/Kfz-Kennzeichenerfassung_und__Bundestrojaner__verfass.de.php

[4] *Podchasov v. Russia*, February 13, 2024, Individual Complaint No.33696/19, https://hudoc.echr.coe.int/eng?i=001-230854 .

[5] Note: Both Art 8 ECHR and Art 10a StGG oblige the state to protect the inviolability of individual communication against dangers, see Merten/Papier, Handbuch der Grundrechte (2009), § 190 Rz 127

the extensive access required, problems arise in regards to the credibility of any evidence obtained by a state trojan. **Ultimately, we also believe that the right to a fair trial in accordance with Article 6 of the ECHR is at risk.**

In our view, the **accompanying legal protection control,** which was essential for the ruling of the Austrian Constitutional Court, is merely **lip service**. Neither has a new institution been created, such as a legal protection senate, nor have the existing mechanisms been equipped with the necessary additional resources or expertise for the continuous monitoring of a highly technical process. The bill also lacks any approach to certifying the software used, as well as audit-proof logging of commands to the state trojan or exfiltrated data.

When encroaching on a fundamental right, the question ultimately always arises as to whether the pursued objectives could not be achieved by a less intrusive means. In our view, the present draft contains such a **lesser means** - namely the **monitoring of unencrypted messages**.

For all these reasons, we clearly reject the current draft law and call for a fact-based security policy discussion in the future, in which experts from the field of IT security research are also involved accordingly.

.

.

Table of contents

NOTES ON THE STATE TROJAN 2024

Previous History

Our organization has been involved in discussions about the legalisation of a state trojan for nearly a decade. We were already involved in the review process for the first draft bill in 2016 with a statement.[6] After the end of the review of the 2016 draft, Federal Minister Wolfgang Brandstetter set up an expert group to "develop proposals for the revision of the current draft, including comparative law aspects"[7] . Although this group included numerous experts in criminal law and criminology, it completely lacked members with technical expertise. This was reflected in the second draft of the law, which did not address the technical objections that were frequently voiced. We also submitted our analysis of this draft during the review process.[8] Following massive criticism from thousands of people and many established institutions, the bill was not passed in the 25th legislative period.

In a third attempt in 2018, the legislature legalized the monitoring of encrypted messages as part of the "surveillance package."[9] However, this legal basis was repealed again in 2019 by the Constitutional Court, which took action following a one-third application by members of the opposition.[10]

In its ruling of 11.12.2019 (Constitutional Court G72/2019), the **Constitutional Court** ruled that the confidential use of computer systems and electronic communications services is a central component of the right to respect for private life in accordance with Art 8 ECHR. The growing importance of computer-based technologies in everyday life makes them a crucial tool for personal development and private life. Data on the use of such systems often provides deep insights into all - even the most intimate - areas of life and allows conclusions to be drawn about users' thoughts, preferences, inclinations and beliefs. In addition, the use of a state trojan often also affects numerous uninvolved persons. For this reason, the **secret surveillance of computer systems is a serious intrusion into protected privacy** and should only take place under the strictest conditions and to protect certain legal interests.

A look at international case law illustrates the central importance of encrypted communication for the protection of privacy and against state surveillance. In the European Court of Human Rights' (**ECtHR**) decision in February 2024 in the case of *Podchasov v. Russia,*[11] the Court clearly emphasized that the decryption of private communications without adequate safeguards constitutes an unlawful interference with the right to privacy under Article 8 of the European Convention on Human Rights. The attempt by the Russian secret service FSB to demand a "backdoor" from the instant messaging service "Telegram," which would have made it possible to decrypt users' messages, was judged by the ECtHR to be a clear violation of fundamental rights. The Court recognized that **encryption is essential for the protection of privacy**, as it prevents not only state authorities but also criminal actors from accessing sensitive personal data.

[6] 350/ME XXVII. GP, Link: https://www.parlament.gv.at/gegenstand/XXV/SNME/6426/

[7] 325/ME XXV. GP Explanatory notes p. 6f

[8] Statement by epicenter.works on the Criminal Procedure Amendment Act 2017 -325/ME, Link: https://www.parlament.gv.at/dokument/XXV/SNME/29496/imfname_666696.pdf

[9] For more information, see here: https://epicenter.works/thema/ueberwachungspaket

[10] "*Constitutional Court largely overturns "security package""* by Redaktion orf.at. 11.12.2019, Link: https://orf.at/stories/3147210/

[11] *Podchasov v. Russia*, February 13, 2024, Individual Complaint No. 33696/19, Link: https://hudoc.echr.coe.int/eng?i=001-230854 .

The current discussion about the state trojan may also be taking place under slightly different circumstances than before, as the legal basis is now in the State Protection and Intelligence Service Act and no longer in the Code of Criminal Procedure, but the essential questions remain the same. Although the current bill attempts to reduce the intensity of the encroachment on fundamental rights and to strengthen legal protection, we believe that the draft falls short of the required standards in both respects..

Legal Protection as Lip Service

As previously explained , in 2019 the Constitutional Court already clearly emphasized how significant a state trojan's interference with the fundamental right to data protection and privacy is, going far beyond any current means of surveillance. The Court therefore also considered special requirements for legal protection to be necessary in order to strike a balance.

The overturned 2018 lawalready contained all the mechanisms provided for in the previous legal protection system, including court approval and the involvement of a legal protection officer.[12] Nevertheless, the Constitutional Court considered the measures to be inadequate. The Court emphasized the **need for "accompanying, effective [...] supervision of the ongoing implementation of this measure",[13] which must be equipped with appropriate technical means and sufficient staff**. This supervision should be carried out by a court or a body with comparable guarantees of independence.

The current draft,[14] still only provides for the Legal Protection Commissioner to ensure this accompanying control. The question therefore arises as to whether the ruling of the Constitutional Court is actually being complied with or whether a new institution should be created that would be suitable for representing the interests of those affected and ensuring that the surveillance measure is implemented in accordance with the law. One possibility would be a **legal protection panel** that is not only staffed by lawyers but **also by IT experts**, so that effective monitoring of the investigative steps can be ensured from both a legal and technical perspective.

However, even if one assumes that no new legal protection institution would be needed, a qualitative assessment of whether controls complying with the Court's decision are possible is not feasible, due to the **lack of an impact assessment** in the current draft. Such an analysis would have to show the additional personnel and resource requirements that the proposed legislation would entail. Such an assessment is therefore essential for planning the actual implementation of the law. However, the fact that the Ministry of the Interior has dispensed with such an assessment casts **doubt on the seriousness of** the planned accompanying control, which is only mentioned as a brief passage in the bill.

We would also like to point out that in the current draft, the measure is only to be approved by individual judges at the Federal Administrative Court. However, our experience in the area of the Code of Criminal Procedure has shown that, in practice, investigative measures requiring approval are often approved too lightly and without thorough examination by detention and legal protection judges at the request of the public prosecutor's office - a practice colloquially known as "**rubber stamping**". Considering the particularly intrusive nature of the planned surveillance measures, it is necessary to reserve the decision on the approval of such intrusive measures to a panel of judges (such as a three-

[12] See Section 137 (1) StPO as amended by Federal Law Gazette No. 27/2018 and Section 147 StPO as amended by Federal Law Gazette No. 27/2018

[13] Constitutional Court 11.12.2019, G 72-74/2019-48, G 181-182/2019-19, margin no. 192; link: https://www.vfgh.gv.at/downloads/VfGH-Erkenntnis_G_181-182_2019-18_G_72-74_2019.pdf

[14] § Section 11 (5) of the draft

judge panel) instead of individual judges. A collegial decision would increase the quality of the review and ensure that the approval is more balanced and appropriate in relation to the interference with fundamental rights.

In addition, it should be noted that the SNG does not provide a legal basis for a possible **complaint by those affected by the surveillance**. The bill merely refers to the possibility of lodging a complaint pursuant to Section 90 SPG - i.e. a complaint due to a violation of the provisions on data protection.[15] It is incomprehensible why there is no explicit basis in the legal text for this very important element of legal protection.

Increased Susceptibility to Misuse

The use of the state trojan is extremely susceptible to misuse, as recent cases show:

In Spain, for example, the secret service used the spyware "Pegasus" to monitor the cell phones of Catalan independence politicians, journalists and activists, among others. Members of the government, such as the Spanish prime minister and defense minister, were also affected.[16] It is still unclear who ordered these actions; it is suspected that parts of the Spanish security apparatus acted on their own authority and without judicial authorization.

Similar incidents occurred in Greece as part of the "Predatorgate" scandal, in which politicians and journalists were monitored by the Greek intelligence service EYP by installing the spyware "Predator" their smartphones.[17] In Poland, "Pegasus" was used against almost 600 people, including opposition politicians and lawyers. These surveillance measures interfered massively with the democratic process and even influenced the election campaign.[18][19]

It is particularly worrying that professional secrecy holders, such as lawyers and journalists, were regularly affected by such surveillance. These professional groups and their communications are particularly protected under Austrian law, as they play a central role in upholding the rule of law and freedom of the press. The surveillance of lawyers undermines the confidentiality of clients' communications with their legal representatives, which in turn interferes with lawyers' professional responsibilities. In the case of journalists, the independence of the media and the protection of sources is jeopardized. This has serious consequences for the protection of fundamental rights and democracy as a whole. **It is therefore incomprehensible why the legislature does not provide for specific provisions to protect these professional groups and their communications**.

These examples clearly show that even in well-established democracies, the use of such surveillance instruments can lead to abuse and violations of fundamental rights. State espionage generally always reduces the security of electronic communication and creates dangerous possibilities for the manipulation and violation of fundamental rights.

[15] See explanatory notes to the ministerial draft 350/ME XXVII. GP, page 8; Link: https://www.parlament.gv.at/dokument/XXVII/ME/350/fname_1650142.pdf

[16] See *"Spain: 2021 spyware attack targeted prime minister's phone"* by Aritz Parra. 02.05.2022, Link: https://apnews.com/article/technology-europe-spain-spyware-9ec1d9ad4a32db1b6002841df612606b

[17] See *"Greece leaves spy services unchecked on Predator hacks"* by Nektaria Stamouli. 07.08.2024, Link: https://www.politico.eu/article/greek-spyware-predatorgate-government-court-report-telephone/

[18] See *"Wiretapping scandal puts PiS in trouble"* by Viktoria Großmann. 19.02.2024, Link: https://www.sueddeutsche.de/politik/polen-pegasus-abhoeraffaere-1.6375787

[19] See *"Poland launches inquiry into previous government's spyware use"* by Shaun Walker. 01.04.2024, Link: https://www.theguardian.com/world/2024/apr/01/poland-launches-inquiry-into-previous-governments-spyware-use

Legal Fiction Fails Due to Technical Reality

The present draft of the state trojan is based on a legal fiction that cannot be implemented in technical reality. The bill suggests the possibility of exclusively monitoring encrypted messages without carrying out a comprehensive online search that invades fundamental rights.[20] However, this idea is technically untenable.[21] Access to communications inevitably requires access to the whole device, as there is no other way to infiltrate surveillance software into messenger services. This not only allows access to photos, documents, location data and never-sent message drafts, but also opens the door for third parties to exploit the security vulnerabilities the state trojan relies on. In practice, the state trojan takes on the role of a "super administrator" on the affected device. In order to be protected against security updates from software manufacturers or to react to updates of the monitored messenger applications, the spy software requires an update function. Thus, the state trojan must be able to download and execut code, which means that misuse can never be ruled out. A clear separation between the monitoring of messages and access to the entire system or locally stored files is not technically feasible. Either data from the messenger application is read, or the entire screen content or keyboard/sound input during the use of certain applications is saved and forwarded. In both cases, however, the state trojan must have already compromised the operating system of the target device and hold administration privileges in order to carry out these operations.[22] The distinction between whether online surveillance and source monitoring is used[23] is also essential to make the subsequent assessment on the impact of the fundamental right to data protection.[24]

The absolute minimum here would be to legally enshrine an independent ex-ante control of the technical systems used depending on their program code and control infrastructure. Certification with published audit reports from an independent body - such as the data protection authority - would be conceivable. Ongoing, efficient legal protection could only be made possible by means of audit-proof logging of all commands to the spy software and the content, telemetry and other data it transmits.[25]

Another problem that is not sufficiently considered in the draft is the enormous technical complexity of a state trojan. Austria will most likely have to rely on external support for its implementation, which will lead to a dependence on foreign intelligence services or private providers. As a rule, neither would provide any insight into how their software operates, leaving Austria in the dark in regards to technical standards, making proper protection of fundamental rights impossible. In both cases, there is also the risk that Austrian interests are subordinated to those of other groups or nations. For instance, private providers regularly cooperate with repressive regimes abroad.[26] In Germany, the managers of a now insolvent provider of state trojan software were indicted in May 2023 in such a case.[27] Last year, the

[20] Cf. explanatory notes to the ministerial draft 350/ME XXVII. GP, page 4

[21] See *"A few thoughts on the "monitoring of encrypted messages"* by Otmar Lendl. 03.09.2024, Link: https://www.cert.at/de/blog/2024/9/ein-paar-gedanken-zur-uberwachung-verschlusselter-nachrichten

[22] See *"Secure Messaging (and current attacks against it)"* by Rene Mayrhofer. 31.08.2024, Link: https://media.ccc.de/v/secure-messaging-and-current-attacks-against-it

[23] See *"Quellen-Telekommunikationsüberwachung zwischen Recht und Technik"* by Mario Martini and Sarah Fröhlingsdorf. 06.02.2021, Link: https://netzpolitik.org/2021/catch-me-if-you-can-quellen-telekommunikationsueberwachung-zwischen-recht-und-technik/

[24] See statement of the Austrian Working Group on Data Retention on amendments to the Code of Criminal Procedure 1975 and the Public Prosecution Act (192/ME XXV. GP), page 3; Link: https://epicenter.works/content/bundestrojaner-stellungnahme-zum-ministerialentwurf

[25] *Ibid.*

[26] See "*New report: FinFisher changes tactics to hook critics*" by Lucie Krahulcova. 13.01.2023, Link: https://www.accessnow.org/new-report-finfisher-changes-tactics-to-hook-critics/

[27] See "*Public prosecutor's office brings charges against FinFisher*" from ZEIT ONLINE. 22.05.2023, Link: https://www.zeit.de/gesellschaft/zeitgeschehen/2023-05/finfisher-spionagesoftware-anklage-muenchen

US government even issued an executive order excluding commercial providers of spy software that promote human rights violations through their business practices from the US market.[28]

It remains unclear how these risks are to be dealt with. We do not believe that the DSN or the bodies entrusted with legal protection by the draft to have the necessary human, technical and financial resources to ensure effective control and security of this dangerous instrument.

State-Sponsored Insecurity - How to Deal with IT Vulnerabilities

If the government plans to use state trojans, this is only possible if specific vulnerabilities in computer systems are maintained and exploited to install and maintain the malware. The current draft even provides for particularly dangerous security vulnerabilities to be exploited, making it possible to take over a device remotely. Such security vulnerabilities are never only accessible to individual (state) actors, but can be discovered and exploited by any third party (other states, cyber criminals).

This creates a conflict of objectives: on the one hand, the state is obliged to report known security vulnerabilities to the manufacturers and to increase the security of the whole population by closing them; on the other hand, it wants to keep these vulnerabilities open and use them for surveillance purposes. By keeping vulnerabilities open, **the state is also clearly violating its positive duty to protect the inviolability of individual communications against threats in accordance with Art 8 ECHR (right to respect for private and family life) and Art 10a StGG (secrecy of telecommunications).**[29] The present bill lacks any consideration as to how a corresponding balance between these interests can be achieved. In summary, the current bill envisions that the state simply ignores the immense risks that have already become apparent in practice. It is precisely this conflict of objectives that is leading to heated debates in Germany.[30]

If the state keeps such vulnerabilities secret, there is a risk that unauthorized third parties will also exploit them. This occurred in the case of the "WannaCry" blackmail trojan, which exploited a security flaw the NSA had used and kept secret for a long time. This vulnerability enabled global cyberattacks that paralyzed hospitals, train stations, airlines and thousands of companies.[31] If this vulnerability had been reported at an early stage, the security of the population and critical IT systems could have been guaranteed. The longer such a vulnerability remains, the greater the risk of exploitation by third parties becomes. The only correct approach would be **to report** these **vulnerabilities to the manufacturers immediately so that they can be closed as quickly as possible**.

Obtaining information about such vulnerabilities is difficult, expensive and often only possible with ethically questionable partners. One option is to purchase information about vulnerabilities on the black market or from software manufacturers. This would ultimately mean that taxpayer money is invested in making IT less secure, while also supporting groups whose business activities are often suspected of contributing to the mass endangerment of the populations around the world. Even when acquiring information, the security flaws are not the exclusive property of a state: the risk of them being discovered by criminals and used for their attacks is real. Google recently published a case in

[28] *Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security*, Link: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/

[29] Merten/Papier, Handbuch der Grundrechte (2009), § 190 para. 127

[30] See "*Dispute over the weak point*" by Florian Flade. 10.01.2024, Link:https://www.tagesschau.de/investigativ/wdr/ueberwachung-software-bundesregierung-100.html

[31] See "*A few theses on current draft laws*" Otmar Lendl. 02.08.2017, Link: https://www.cert.at/de/blog/2017/8/blog-20170731130131-2076

which the same vulnerabilities used by spyware manufacturers were exploited by hackers from the Russian foreign intelligence service to attack the systems of a foreign state and its population.[32] According to Google, it is almost impossible that the attack code was found by Russia independently; they either bought or stole the knowledge from the spy software manufacturers.

The use of state trojans is therefore not just a means of surveillance, but above all a means of creating uncertainty and threat scenarios in IT systems. As a result of the state trojans inherent reliance on security flaws, the government proposal to implement the NIS2 Directive in Austria must also be considered. This creates an obligation to report security vulnerabilities to government agencies, even at a time when they still pose an active threat to IT systems.[33] In Germany, the Federal Office for Information Security, which is responsible for handling such vulnerability reports, was caught helping to implement a state trojan.[34] Spyware and state hacking create a reversal of interest in the state's duty to protect, where the responsible handling of security vulnerabilities and the necessary trust in state institutions are systematically undermined.

Threat to Austria as a Business Location

In this context, we are particularly critical of the duties of cooperation and confidentiality[35] that are provided for service providers in the current draft of the SNG. The obligations to cooperate are only described in very general terms, which allows for a wide range of potential requirements. This could mean, for example, that large service providers are forced to act as handlers for the DSN. **Instead of guaranteeing their customers security, they would be forced to allow insecurity** by supporting government surveillance measures.

The current obligation to cooperate could be interpreted in various ways. In the worst case, the provision allows for bussinesses to be forced to create security vulnerabilities in specific products or systems. It could also be interpreted in such a way that the manufacturer is required to preserve known security vulnerabilities. Finally, the bill could also be used to force a company (e.g. telecommunications company or device manufacturer) to aid in infecting a surveillance target. All of these interpretations of the provision in question represent massive violations of fundamental rights, would undermine the business freedom of the related companies, and would ultimately result in an **irreparable loss of** public **confidence** in domestic companies.

We believe that the planned confidentiality and blanket duties to cooperate are not clearly defined, leaving a massive lack of legal protection. We therefore urgently recommend that the provisions in question be removed.

Least Intrusive Means?

In its 2019 ruling, the Constitutional Court emphasized that the right to confidentiality of personal data, as enshrined in Section 1 para. 1 of the Data Protection Act, is also infringed upon by the possible use of the state trojan. Even if a measure is designed in accordance with Art 8 ECHR, the

[32] Cf *"The tricks of the "Bundestrojaner" have fallen into the hands of Moscow"* without author on derstandard.at. 01.09.2024, Link: https://www.derstandard.de/story/3000000234720/die-tricks-des-bundestrojaners-sind-in-die-haende-moskaus-gefallen

[33] Art 29 f NIS-2 Directive 2022/2555, further information at: https://epicenter.works/content/nis2-verpasste-chance-fuer-oesterreichs-it-sicherheit and https://www.parlament.gv.at/aktuelles/pk/jahr_2024/pk0785

[34] See "*BSI programmed and actively worked on the state Trojan, but denies cooperation*" by Andre Meister. 16.03.2015, Link: https://netzpolitik.org/2015/geheime-kommunikation-bsi-programmierte-und-arbeitete-aktiv-am-staatstrojaner-streitet-aber-zusammenarbeit-ab/

[35] § Section 11 (2) and (3) of the draft

more far-reaching criteria of Section 1 (2) Data Protection Act must still be examined. These include, in particular, the existence of an important public interest, appropriate privacy safeguards, and only using the least intrusive means to achieve the intended purpose.[36]

In this context, the question arises as to whether the state trojan is truly the least intrusive means. The investigating authorities already have a range of other, less intrusive measures at their disposal, such as the confiscation and analysis of devices, the retrieval of data from cloud service providers (backups) and traditional surveillance.

It is particularly noteworthy that the current discussion has barely touched on the fact that this draft also creates a **basis for the DSN to monitor unencrypted communication** for the first time.[37] Previously, the DSN has only been able to monitor traffic data,[38] but now access to unencrypted content is to be legalized as well. Considering that the current debate on encrypted communications was actually sparked by a case solved by monitoring unencrypted communications,[39] it seems incomprehensible why the legislature does not first examine if the monitoring of unencrypted communication is sufficient to meet the specific objectives of the DSN. All three previously foiled attack plans in recent years were discovered by monitoring unencrypted Telegram communication.[40]

Thus, the question of whether the surveillance of unencrypted communication is not already the least intrusive means should be deliberated before further-reaching encroachments on fundamental rights, such as the use of the state trojan, can be justified. Extending surveillance powers to unencrypted communications while providing appropriate legal protection would arguably fulfill the desired security goals while avoiding the myriad of previously outlined negative societal consequences.

Utilization of Evidence

As previously explained, the use of malware to monitor messages requires extensive control over the target operating system, making it impossible to determine whether or not information on the device has been externally manipulatedPotential evidence could thus **be planted by third parties**, as the extensive access rights also allow changes to be made to stored files. Regardless of if information is manipulated or not, the mere fact that evidence has been obtained from a demonstrably hacked device is enough to significantly weaken the quality of evidence. The collection of such evidence, which is susceptible to manipulation, is contrary to the principles of a fair trial in accordance with Art 6 ECHR[41] and jeopardizes its implementation from the outset.

[36] Constitutional Court 11.12.2019, G 72-74/2019-48, G 181-182/2019-19, margin no. 177

[37] § Section 11 (1) no. 8 of the draft

[38] Explanatory notes on the ministerial draft 350/ME XXVII. GP, page 3

[39] See "*The pippification of IT security law*" by Nikolaus Forgo. 20.08.2024, Link: https://www.derstandard.at/story/3000000232965/die-verpippisierung-des-it-sicherheitsrechts.

[40] See *"Expert on messenger surveillance"* ORF III aktuell. Aired on 14.08.2024, link: https://on.orf.at/video/14238449/15700522/experte-zu-messanger-ueberwachung Cf. *"Suspect announced terrorist attack on Vienna Pride in IS chat"* by Jan Michael Marchart and Fabian Schmid. 21.06.2023, Link: https://www.derstandard.at/story/3000000175546/verdaechtige-kuendigte-terroranschlag-auf-wiener-pride-in-i; Cf. *"Viennese jihadist planned attack: Ripe for punishment, but not for incarceration"* by Jan Michael Marchart. 18.12.2023, Link:https://www.derstandard.at/story/3000000200089/wiener-jihadist-plante-anschlag-reif-fuer-strafe-aber-nicht-fuer-einweisung.

[41] ECtHR; *Jalloh v. Germany*, July 11, 2006, individual application no. 54810/00, https://hudoc.echr.coe.int/eng?i=001-139332

We also believe the provisions on dealing with accidental discoveries must be improved. It must be ensured that accidentally discovered evidence is only used if all the conditions under which surveillance of encrypted messages could have been ordered were met.[42]

Data Security and Quality Management

Given the complexity and the risks associated with the state trojan, it is striking that data security and quality management take up very little space in the draft. Although it is logical that the law itself does not contain all the exact requirements for a software that is yet to be procured, there should at least be broad outlines of a security concept that addresses the specific risks associated with the use of a state trojan. For example, providing criteria for the procurement, approval, and testing process is vital. Similarly, defining in advance how the use of the software can be monitored (through regular audits by an independent and technically competent body, storage of audit-proof log files, etc.) would also be important.

Alternatively, the law could only contain the broad requirement to create a safety or quality management concept, thus leaving the specific requirements to be issued by ordinance. The German state trojan law follows this model, with the "Standardized Service Description"[43] specifying the law's requirements andprocesses.

[42] Cf. statement of the Institute for Austrian and European Business Penal Law on the draft of a federal law amending the State Protection and Intelligence Service Act. Link: https://www.parlament.gv.at/PtWeb/api/s3serv/file/58361fe5-e400-4a05-af97-f9de114a9767

[43] See "*Quellen- und Online-Durchsuchung*" without author Bundeskriminalamt Deutschland. Accessed on 03.09.2024, Link: https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html

NOTES ON FURTHER PROVISIONS

Re Section 11 para. 1 no. 5 (IMSI Catcher)

This provision is intended to enable the use of the so-called IMSI catcher in the SNG, as is already the case in the StPO and the SPG.

As already explained elsewhere,[44] the problem with using an IMSI catcher is that its actual abilities far exceed what the underlying legal basis allows. While the bill only provides for the current location or IMSI number of a cell phone or tablet to be collected, the IMSI catcher can also intercept the content of calls without the cooperation of the mobile phone provider being required. The measure is undetectable by subscribers as well as the provider. It is therefore urgently necessary to create legal, technical and organizational safeguards to ensure that it is used in accordance with the law. However, the draft does not provide for a clear authorization for an implementing regulation governing its use.

One possible organizational measure could be the introduction of a dual control principle for data collection. On a technical level, it would make sense to implement an audit function that checks whether the IMSI catcher has been used exclusively for legally permissible purposes. In its current form, however, the regulation **does not meet the requirement of determination under fundamental rights** and thus opens the door to the arbitrary use of this technology.

In its ruling 12 Os 93/14i on radio cell analysis, the Austrian Supreme Court (OGH) stated that the principle of proportionality must be upheld by limiting the duration of such measures. This is intended to ensure that the privacy of communications of uninvolved persons is only interfered with to the extent that it is unavoidable for a promising investigative step and remains justifiable in view of the number of persons affected and the seriousness of the crimes to be solved. In view of the wide range of such interventions and the potentially large number of persons affected, stricter controls are necessary to prevent abuse.

Re section 11 (1) no. 8 (interception of unencrypted messages)

In principle, we welcome that the DSN could monitor unencrypted messages for certain purposes under the current bill. Based on the information available to us, it can be deduced that this ability alone would already be sufficient to cover the situations the present bill aims to prevent. Essentially, the DSN is granted measures already available to other Austrian law enforcement authorities, although the DSN must follow stricter requirements with regard to the material threshold for intervention and necessity. Simultaneously, we consider the effective supervision of these measures to be essential, and would like to point out - as already mentioned in the general section - the complete lack of an impact-oriented impact assessment.

[44] Statement by epicenter.works on the Criminal Procedure Amendment Act 2017 -325/ME, page 6; Link: https://www.parlament.gv.at/dokument/XXV/SNME/29496/imfname_666696.pdf