

Ninth State Treaty amending state treaties on media law

Subject: Use of technical means in media supervision

Proposal for anchoring a standard in the Interstate Media Treaty

§ 109a Use of technical means in supervision	Notes
(1) The state media authorities may use technical means to investigate infringements of the law, as defined by § 109 of this State Treaty and § 20 JMStV, that include text-, image-, audio- and automatically compare video content from broadcasting and telemedia for potential violations. Sentence 1 also includes content in broadcasting and telemedia that is subject to access restrictions.	Paragraph 1 provides for the fundamental admissibility of an automated research and examination of content for potential infringements of the law. An automated comparison also includes the use of AI-based systems, to which the requirements of the AI Regulation apply, in addition to the data protection requirements of Paragraphs 2 et seq. The possibility of using technical means provides for an efficient and effective independent media oversight and can also contribute to a higher level of employee protection in the handling of sensitive material. Infringements of the law are limited within the scope of the authorisation to use such technical means to those that are also subject to supervisory measures by the state media authorities pursuant to § 109 MStV or § 20 JMStV. The automated comparison will also be limited to broadcast and telemedia content. Only these services fall within the scope of the Interstate Media Treaty and the Interstate Treaty on the Protection of Minors in the Media, and as such are subject to the supervision of the state media authorities. At the same time, this limits the comparison with content that is made 'public' by a provider, since both broadcasting and telemedia are journalistic offerings which, in contrast to individual communication, are aimed at an indefinite number of users. Access restrictions as defined by Sentence 2 are, insofar as they are to be assessed as broadcasting or telemedia, only accessible behind an age verification system or paywall after registering or creating a user account (for example).
(2) The information referred to in the text-, image-, audio- and video content, including special categories of personal data as defined by Article 9(1) of Regulation (EU) 2016/679, may be processed within the framework of the automated comparison pursuant to Paragraph 1, insofar as and to the extent that this is necessary to be able to make a final assessment of the content. An automated comparison based on specific personal data is not permitted.	Infringements of the law as defined by Paragraph 1 are directed at general elements of the offence, not at specific persons, such that the collection of personal data is generally not the focus, nor should it be. Nevertheless, the compared content may unavoidably and necessarily contain personal data. This personal data may also constitute special categories of personal data. In particular, visual materials may, for example, provide information about racial and ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, or contain health data or data relating to a natural person's sexual life or sexual orientation. The processing of this data is therefore only permitted within narrow limits. The processing, and in

	particular the collection, of data is permissible only if it arises from the compared content itself and is necessary for processing the content under supervisory law. Such data processing is permissible on the basis of Art. 9(2)(e) GDPR if the data have been made 'obviously public' by the data subject themselves. However, when it concerns the published data of third parties, the balancing required under Art. 9(2)(g) GDPR ('significant public interest') is largely determined by the close inseparable connection with the content to be reviewed and the high-level protected interests at stake. Since an assessment of content without its overall context is not possible, an infringement cannot be determined. Even and especially in particularly sensitive cases, e.g., sexual acts, measures, in particular prohibition, deletion- and blocking orders issued by the state media authorities, also serve the interests of these third parties. Insofar as it is possible to separate personal data and thus make its collection unnecessary, particularly sensitive data must not be stored. 'Profiling' is not part of the comparison process provided for in Paragraph 1 and would be inadmissible. In addition, the exclusion of a comparison based on specific personal data, i.e., data relating to a specific person, is explicitly stated.
(3) Where a potential infringement of the law as defined by Paragraph 1 is detected using technical means, the following additional personal data relating to the potentially infringing content may be processed using that technical means, provided that such data are necessary for the purposes of Paragraph 4: Provider data, including information pursuant to § 18, web address of the content, date of publication and time of data collection, geographical location, links and interactions with the content.	If a potential infringement of the law, which is subject to supervisory measures under § 109 MStV and/or § 20 JMStV, is detected by the tool, further personal data may be collected and processed in addition to the content itself, provided that this is necessary for subsequent supervisory measures.
(4) If the technical means detects a potential infringement of the law as defined by Paragraph 1, it must be verified without delay by a natural person whether this can be confirmed; if this is not the case, the processed personal data must be deleted without delay. A deletion pursuant to Sentence 1 must take place no later than 30 days, even if no review could be carried out by then.	Collected data must be subjected to an immediate human review. In the absence of a concrete suspicion of a legal violation, data must be deleted immediately. If no review takes place, data must be deleted after a maximum of 30 days.
(5) Those involved in the processing of special categories of personal data must be made aware of the special need for protection of such data. Suitable technical and organisational measures must be taken to ensure that it can be subsequently verified whether and by whom personal data as defined by Paragraphs 2 and 3 have been entered, changed or removed. The general data protection regulations, in particular those concerning the security of personal data, remain unaffected.	Guidelines for data security are defined. Other data protection regulations (e.g., issues of transfer to third countries, security of personal data, etc.) remain unaffected.
(6) If, after review in accordance with Paragraph 4,	In cases of concrete suspicion of an infringement of

there is a concrete suspicion of an infringement of the law, the personal data may be processed for the purpose of carrying out supervisory measures pursuant to § 109 of this State Treaty and § 20 JMStV, as well as for the prosecution of administrative offences pursuant to § 115(1) of this State Treaty, and § 24(1) and (2) JMStV. If there is suspicion of a criminal offence related to the elements of the offence under § 4(1) or (2)(1) JMStV, or a criminal offence under § 23 JMStV, personal data may also be forwarded to other competent authorities if this is necessary for the investigation and prosecution of these criminal offences. A use for other purposes is not permitted. Personal data must be deleted immediately if it is no longer required for the implementation of supervisory measures or the prosecution of administrative offences, at the latest after 6 months, provided that no supervisory proceedings are pending by then.	the law, personal data may be used for supervisory measures and the prosecution of administrative offences. The statute of limitations for administrative offences forms the limit of permissible data storage. In addition, deletion obligations are also provided for stored data for which no proceedings have been initiated. If there is suspicion of a criminal offence based on the elements of the offence under § 4(1) or (2)(1) or § 23 JMStV, required data may be passed on to the law enforcement authorities.
(7) Technical means as defined by Paragraph 1 shall be based on suitable algorithms, models and training data. The technical means must be validated before use and regularly thereafter. A training with anonymised data is permitted. The use of personal data for the purpose of training technical means for use in accordance with Paragraph 1 is not permitted; exceptions apply to personal data required pursuant to Paragraph 2(1) and concerning figures in the public eye, insofar as pseudonymisation is not effective or is disproportionate. Anonymisation or pseudonymisation of personal data before its deletion pursuant to Paragraph 4, Sentence 1 2. The use of a clause for the purpose of training technical means is permissible, provided that the data is necessary for the investigation of infringements of the law as defined by Paragraph 1. Before using technical tools, a data protection impact assessment must be carried out in accordance with § 35 of Regulation (EU) 2016/679.	Requirements for technical means and their verification are specified in more detail. In particular, a regular validation is prescribed and specifications for training data are defined. Training with personal data is therefore generally prohibited. However, in order to ensure the functionality and accuracy of such a tool while also minimising data usage, personal data must be able to be used for training purposes where necessary. Sentence 3 provides for a corresponding exception. This also extends to required data on figures in the public eye who, particularly due to historical references, can be relevant reference points for the search. Before the deletion of personal data pursuant to Paragraph 4, Sentence 1 2. The clause states that anonymisation of personal data for the purpose of training of technical tools is permissible. However, this is subject to the condition that the data is necessary for using the tool, i.e., the detection of infringements of the law pursuant to Paragraph 1. Anonymisation processes must comply with the current standards.
(8) Details concerning the type, purpose and use of technical means pursuant to Paragraph 1 will be regulated by the State Media Authorities by means of a joint statute. The use of technical means must be documented; key results of the use must be published annually in a report. As part of supervisory measures, the use of technical means must be disclosed to the provider concerned.	Through a statutory authorisation, committees are involved in the fundamentals of the design and use of technical means; the statutes may, in particular, specify areas of use, operating hours, or define -cycles, functionality and categories of search criteria in more detail. A common set of regulations ensures that the state media authorities operate according to uniform standards.
(9) Providers of online platforms as defined by Regulation (EU) 2022/2065 shall, at the request of the competent state media authority, provide suitable interfaces for the use of the technical means referred to in Paragraph 1, insofar as this is technically and economically feasible. Only data as defined in Paragraphs 2 and 3 may be made available via the	In addition to the obligation of providers to allow supervision of their services, as stipulated in § 109(4) MStV and § 21(3) JMStV, a specific interface obligation for the use of technical means is introduced. This obligation addresses online platforms and thus telemedia services that, unlike content providers and media platforms, do not offer content

interface. § 109(4) and § 21(3) of the Interstate Treaty on the Protection of Minors in the Media apply accordingly.	or overall services for which they are solely responsible. These are essentially media intermediaries. These telemedia services are subject to the liability regime of Regulation (EU) 2022/2065 and are therefore regularly exempt from liability for the information provided by their users. These guidelines remain unchanged. By requiring media regulators to provide a required interface, access to content for which third parties are responsible, and thus an oversight of this content or content providers, is ensured. Only the relevant, publicly accessible data mentioned in Paragraphs 2 and 3, but not contract data or data stored behind accounts, may be made available via the interface. Access must be granted free of charge, as in the cases of § 109(4) MStV, and § 21(3) JMStV.