Deliberation 2021-045 of April 15, 2021 National Commission for Computing and Liberties Nature of the deliberation: Opinion Legal status: In force Date of publication on Légifrance: Wednesday May 19, 2021 Deliberation No. 2021-045 of April 15, 2021 providing an opinion on Articles 13 bis and 13 ter of the draft law on the prevention of acts of terrorism and intelligence (request for opinion no. 21007082) The National Commission for Computing and Liberties, Referred by the Ministry of the Interior to a request for an opinion concerning a draft law relating to the prevention of acts of terrorism and intelligence; Having regard to law n° 78-17 of January 6, 1978 as amended relating to data processing, files and freedoms, in particular its article 8; After hearing the report of Mrs Sophie LAMBREMON, commissioner, and the observations of Mr Benjamin TOUZANNE, government commissioner, Issues the following opinion The Commission was seized urgently, on April 2, 2021, on the basis of section 8 -4°-a) of the amended law of 6 January 1978, articles 13 bis and 13 ter of the draft law on the prevention of acts of terrorism and intelligence (hereinafter the draft law). The Commission stresses that the issues associated with the planned amendments are of a very distinct nature, and do not have the same sensitivity from the point of view of the right to respect for private life and the protection of personal data. In particular, it considers that all of these provisions contribute to the implementation of surveillance measures likely to significantly affect the fundamental rights of the persons concerned. The Commission recalls in this respect that such attacks can be justified if they are limited to what is strictly necessary, with regard to the legitimacy of the objectives pursued, which constitute national security and the safeguard of the fundamental interests of the Nation. The developments envisaged by the aim, on the one hand, to supervise the implementation of a new intelligence technique allowing, by means of proximity capture devices, the interception of correspondence transiting by satellite. On the other hand, the proposed changes regulate the exchange of information between the judicial services and the intelligence services, as well as with the National Information Systems Security Agency (ANSSI). On the implementation of a new intelligence technique for interception of correspondence (article 13 bis) On the principle of experimenting with this new technique Article 13 bis of the bill provides a framework for the implementation of a new intelligence technique, which aims to enable intelligence services to intercept, by means of a proximity capture device, correspondence sent or received transiting by satellite. It provides for an experimental period of four years. As a preliminary point, the Commission notes that the implementation of such a device is similar to the so-called IMSI-catcher technique, currently governed by Article L. 852- 1-II of the Internal Security Code (CSI), and on which it has already ruled in its deliberation n° 2015-078 of March 5, 2015. It recalls that this type of intelligence technique is likely to allow the collection systematic and automatic data relating to people who may

have no connection or a simple geographical proximity to the individual actually monitored. In the absence of technical measures making it possible to filter the targeted correspondence and to access only useful data concerning a person identified as being the subject of targeted surveillance, it will be a question of making it possible to collect, in an undifferentiated manner, a potentially large volume of data, which may relate to people completely unrelated to the intelligence mission, including people whose correspondence is protected by law. The Commission invites the Government, during the experiment, and if technically feasible, to implement such filtering measures as far upstream as possible. The potential invasion of the privacy of individuals is therefore particularly strong. Thus, as the Commission pointed out in its aforementioned deliberation, it considers that such measures are only justifiable if they prove to be strictly necessary for overriding objectives in the general interest, in the alternative to other more targeted, and whether they are accompanied by guarantees and effective monitoring methods making it possible to limit infringements of the fundamental rights of the persons concerned. The Commission notes that the launch of the experiment envisaged by the Government will be decided by Parliament at a time when many elements remain uncertain. It includes documents that have been transmitted to it that, the development of satellite transmissions escaping the traditional modes of surveillance, the implementation of this new technique must make it possible to adapt the techniques of capture to the significant evolution of the modes of communication. While the Ministry has specified that it considers the current legal framework to be inadequate for intercepting these new forms of communication, the Commission points out that it appears that the technical methods that will be used to capture these transmissions have not yet been fully defined. Under these conditions, it welcomes the principle of conditioning the implementation of this technique on experimentation, insofar as this could make it possible to assess the proportionality and effectiveness of these measures before considering their sustainability. The Commission considers, however, that in view of the invasion of privacy caused by this type of interception of correspondence, the legislator must subject the experiment to explicit conditions guaranteeing the strict proportionality of the invasion of privacy. In this respect, the Commission underlines that uncertainties remain both on the volume of transmissions which could escape the intelligence services, via current techniques, due to the development of these new forms of satellite communications, and on the methods and effectiveness of the techniques allowing the interceptions. The assessment of the proportionality of the interference is therefore uncertain and evolving. Some of the data intercepted may be encrypted and this point should also be taken into account when assessing the implementation of this technique. The Commission therefore considers that, if it were to prove, after first experimental tests, that the operational necessity has been

overestimated or that the technical methods make it impossible or disproportionate to resort to such interception of correspondence, it would be appropriate to interrupt the experiment before the expiry of the four-year period. The law could specify that the effective use of this new technique will only be possible as long as its operational usefulness is not denied, either if this type of satellite transmission did not experience the expected development, or if the technical methods of interception turned out to be unsatisfactory. In this context, the Commission asks that the draft law provide for an interim report to be carried out and sent to Parliament, under the same conditions as that which will have to be carried out, in accordance with the draft article 13 bis, before the end of the experiment. The Commission also recalls that the National Commission for the Control of Intelligence Techniques (CNCTR) may, in accordance with Articles L. 833-6 and L. 833-6 of the CSI, carry out this control during the experiment and in particular recommend as such the Prime Minister to interrupt or suspend the experiment, if necessary by seizing the specialized formation of the Council of State, if the conditions laid down by law for its conduct were no longer met. Finally, it underlines that in order to accurately assess the benefits that would be derived from the device, the assessment referred to in the aforementioned article must at least relate to a certain number of characteristics, in particular operational, relating to this technique. The Commission more particularly encourages the Ministry to quantify the volume of data collected, and in particular those concerning persons not subject to the authorization. It also considers that quantitative elements on the efficiency of this technique, as well as the duration of the use of these capture devices, should also appear in the report submitted to Parliament. On the conditions for implementing the technique and the safeguards provided for in Article 13 bis of the draft law In general, the Commission considers that experimentation can only be accepted if sufficient safeguards are provided to limit the invasion of privacy to what is strictly necessary. In this regard, it notes that the bill provides guarantees that are partly similar to those provided for in the provisions of Article L. 852-1 of the CSI governing IMSI-catchers. The Commission nevertheless emphasizes that some of the methods of implementing this technique differ, taking into account, on the one hand, the specificities which are specific to it, and, on the other hand, the choice made by the Ministry not to include all guarantees associated with the IMSI-catcher device. Firstly, the Commission notes that the implementation of this technique is subject to authorization by the Prime Minister, after consulting the CNCTR, and that moreover the data collected in this framework are centralized by the Interministerial Control Group (GIC). It stresses that article 13 bis of the bill provides that data unrelated to the initial authorization must be immediately destroyed and cannot give rise to any exploitation, an element which it considers essential to the balance of the system. Finally, it notes that the maximum

number of interception authorizations in force simultaneously is set by the Prime Minister, after consulting the CNCTR, and that the operations of transcription and extraction of intercepted communications, to which the aforementioned commission has permanent, complete, direct and immediate access are carried out within the GIC.Secondly, the Commission notes that, given the specificities associated with the development of this new intelligence system of specific guarantees. First of all, the Commission notes that the data will be encrypted as soon as it is captured by an asymmetric encryption in the event that immediate centralization is not possible. In this respect, it recalls that the methods used must comply with appendix B1 of the general security reference system (RGS) and that the private keys must be subject to security measures aimed at guaranteeing that their use is strictly limited to authorized persons. In addition, article 13 bis of the bill provides that the use of this new technique may be authorized when this interception cannot be implemented under the conditions provided for in I of article L. 852-1 of this code. In this respect, the ministry specified that this hypothesis corresponds to the cases in which it will be impossible to implement a security interception on the basis of the aforementioned article, in particular because of the difficulties in requisitioning certain types of operators. The Commission considers that these methods constitute a guarantee making it possible to rule out the systematic nature of the implementation of this technique, and thus make it possible to limit its use to what is strictly necessary. In this respect, it calls for strict control of the subsidiarity of this technique and considers that Article 13 bis could be supplemented in order to specify the criteria justifying the use of this technique, which is much more intrusive than targeted interception. Commission takes note of the details provided by the Ministry on the geographical scope of the implementation of these recordings. If the current devices have a reduced range, the objective attached to the implementation of this technique will be to reduce as much as possible the area concerned around the target covered by the authorization issued by the Prime Minister and thereby to increase the specificity of the data collected. The Commission considers that these elements contribute to the overall assessment of the proportionality of the mechanism in question. Thirdly, the Commission considers that some of the methods of implementing this technique call for specific comments. On the one hand, the Commission notes that this technique can be implemented for all the purposes provided for in Article L. 811-3 of the CSI. Given the challenges previously mentioned with regard to the collection of data using this type of technique, and more particularly its experimental nature, the Commission wonders about such a scope. If the Commission does not question the interest which would ultimately result from the implementation of this technique for all the purposes pursued by the intelligence services, as is the case for common law security interceptions existing today, it considers that the uncertainties, both technical

and operational, relating to the implementation of this technique, and the very specific invasion of privacy it brings, should lead the Ministry to consider its development in an experimental framework for the sole purposes of interest the most imperative, and considered to be the most serious. Finally, it recalls that concerning IMSI-catchers, the conditions for es of the technique envisaged, the limited use of certain purposes relating to the prevention of particularly serious breaches of public order had been taken into account by the Constitutional Council (decision no. 2015-713 DC of July 23, 2015) to declare these provisions comply with the Constitution. On the other hand, the bill provides that the authorization to use this technique is issued for a maximum period of thirty days, renewable under the same conditions. The Commission notes that this duration is less than that applicable to interceptions of correspondence governed by ordinary law and governed by Article L. 852-1-I of the CSI, carried out at the request of operators, which is four months. On the other hand, it is significantly longer than the authorization period for IMSI-catchers, which is forty-eight hours. To justify this duration, the Government argued that the IMSI-catcher is a completely derogatory technique, corresponding to certain use cases, in a technical environment where security interceptions are possible. The planned experiment consists of allowing, on a subsidiary basis, security interceptions to be carried out for communications for which the requisitions currently practiced are not possible. In this context, the ministry estimates that the time required to carry out such a security interception is well over forty-eight hours. The Commission takes note of these explanations, which led the Government to set the duration of authorizations at a quarter of that practiced for current security interceptions, but recalls that it asks, on the one hand, that the technique used allow, as much as possible, to carry out upstream filtering (within the capture equipment if possible), of correspondence unrelated to the surveillance measure, on the other hand, that the proportionality of the invasion of privacy caused by the experience is regularly reassessed. On the exchange of information between the judicial authorities and the intelligence services (article 13 ter) Article 13 ter of the draft law regulates, for certain investigation or investigation procedures and by derogation from the secrecy of the investigation, the possibility for the public prosecutor of Paris (or, where applicable, the investigating judge), to communicate to the intelligence services elements of any kind appearing in s these procedures and necessary for the exercise of the missions of these services. As a preliminary point, the Commission notes that Article 706-25-2 of the Code of Criminal Procedure (CPP) already provides that the public prosecutor Anti-terrorist Republic, for investigation or investigation procedures opened on the basis of one or more terrorist offences, may communicate to the specialized intelligence services, on its own initiative or at the request of these services, elements of any nature appearing in these procedures and necessary for the exercise of the missions of

these services in terms of the prevention of terrorism. the provisions referred to, insofar as they allow the transmission of personal data, must be carried out in compliance with the principles relating to the protection of this s data, and more specifically those relating to the proportionality and lawfulness of the processing. Firstly, the Commission takes note of the justifications provided by the Ministry according to which it appears necessary to promote exchanges between the judicial authority and the intelligence services on organized crime and the fight against cybercrime. In this respect, it notes that the scope of offenses covered by the draft law appears to be very broad due to some of the criminal offenses to which it refers (for example with regard to the offenses of drug trafficking), without however the cases of use corresponding to such a possibility are not particularly identified and have been brought to its attention at this stage. Consequently, it wonders about the scope precisely targeted by article 13 ter of the bill. Secondly, the bill specifies that this communication can take place on the initiative of the public prosecutor or the judge of instruction, or at the request of the intelligence services. In this regard, the ministry has indicated that there is no obligation to transmit. If it takes note of this element, the Commission considers that the draft law should be clarified in order to expressly mention the optional nature, for the judicial authorities, of transmitting such data. Finally, with regard to the possibility, for the authorities authorities, to transmit information to ANSSI, if the Commission makes the same observations as previously developed, it considers that, given the missions of this agency, the nature of the information likely to be communicated to it will necessarily be intended to be more restricted .It nevertheless calls for strict control of the procedures for implementing this possibility.President Marie-Laure DENIS