Deliberation 2021-053 of May 3, 2021 National Commission for Computing and Liberties Nature of the deliberation: Opinion Legal status: In force Date of publication on Légifrance: Tuesday May 18, 2021 Deliberation No. 2021-053 of May 3, 2021 providing an opinion on Articles 11 quinquies, 11 sexies and 11 septies of the draft law on the prevention of acts of terrorism and intelligence (request for opinion no. interior of a request for an opinion concerning Articles 11 quinquies, 11 sexies and 11 septies of a bill relating to the prevention of acts of terrorism and intelligence; Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (general regulation on the protection of given es); Considering the modified law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms, in particular its article 8-4°-a); After having heard the report of Mrs Sophie LAMBREMON, commissioner , and the observations of Mr Benjamin TOUZANNE, Government Commissioner, Issues the following opinion: of January 6, 1978 as amended, Articles 11 quinquies, 11 sexies and 11 septies of the bill relating to the prevention of acts of terrorism and intelligence (hereinafter the bill). These articles are essentially intended to take into account the French Data Network and others decision rendered by the Council of State ruling on litigation on April 21, 2021 (No. 393099, 394922, 397844, 397851, 424717, 424718). The Commission emphasizes from the outset that this decision, which follows a referral by the Council of State to the Court of Justice of the European Union (CJEU) for a preliminary ruling, raises significant issues both in terms of public freedoms, and in particular the preservation of people's private life, and the effectiveness of public action to guarantee the fundamental interests of the Nation, public security and the repression of offences. These decisions and their implementation contribute to defining a balance between these imperatives, which constitutes a societal choice and a political choice, which it is up to Parliament to weigh, perfect and specify. In its decision, the Board of State has ordered the Prime Minister to repeal, within six months, Article R. 10-13 of the Post and Electronic Communications Code (CPCE) as well as Decree No. 2011-219 of 25 February 2011 relating to the storage and communication of data enabling the identification of any person who has contributed to the creation of online content. The Council of State also noted that the provisions aimed at allowing the implementation of intelligence techniques, without prior control by an independent administrative authority endowed with the power of assent or a court, except in cases of duly justified urgency, had to be cancelled. 'part of these provisions must be specified by regulation and specify in this respect that it intends to carry out a detailed examination of this system without this prejudging its assessment of compliance with the principles relating to the protection of personal data' regarding the conditions for the

effective implementation of these provisions. It nevertheless regrets having to decide under urgent conditions. extreme ence on such developments, given the challenges associated with the generalized and undifferentiated collection of data relating to electronic communications and the substantial impacts on the privacy of the persons concerned which result therefrom. On the modification of the provisions relating to the retention of data relating to electronic communications by operators (article 11 quinquies of the bill)The draft law provides for the modification of article 34-1 of the CPCE which organizes the system for the retention of data relating to electronic communications by operators , to provide, by way of derogation from the principle according to which these operators erase or render anonymous without delay the connection data relating to the communications of their subscribers, the cases in which this obligation may be waived. to the identity of users, as well as technical data allowing them to be identified, or relating to the connection terminal equipment used five years after the end of validity of his contract; the other information provided by the user when subscribing to a contract or creating an account, as well as information relating to payment, for a period of one year; the technical data enabling the user to be identified or relating to the terminal connection equipment used, for a period of one year. While the Commission notes that the Court of Justice and the Council of State have accepted the possibility of storing in a generalized and undifferentiated manner data relating to communications relating to the identity of the persons concerned, in particular insofar as their storage is considered likely less interference with the privacy of these persons, the proposed provisions call for the following observations. Firstly, the bill provides that a decree in Council of State, issued after consulting the computing and freedoms, determines, according to the activity of the operators and the nature of the communications, the information and categories of data kept pursuant to this article. The Commission notes that the reference to technical data enabling the user to be identified or relating to the terminal connection equipment used is particularly broad. While it notes that the IP address may in particular be kept in this respect, it recalls that only the data necessary for the purposes pursued by such storage must be kept by the operators. In this respect, it also recalls that the CJEU considered that the retention of this data should in particular, for purposes other than those relating to national security, be temporarily limited to what is strictly necessary. It also points out that the retention of this type of data cannot be justified for a wide spectrum of purposes and in particular the pursuit and investigation of any criminal offence. In this respect, if the Council of State considered that the legislator was not required to list the offenses falling within the scope of serious criminality and for which the retention of this data would be justified (which will in any case be controlled by the criminal judge), the Commission considers that the bill should specify the primary purposes for which these data should be kept by the

operators.Secondly, the bill provides that the data kept and processed under the conditions defined in II bis to V relate exclusively to the identification of the persons using the services provided by the operators, to the technical characteristics of the communications provided by the latter and to the location of the terminal equipment. In this regard, the Commission notes that given the purposes for which they are processed, the data stored under the conditions defined in II bis of Article 34-1 of the CPCE cannot relate to the location of terminal equipment. It therefore invites the Ministry to clarify the aforementioned provision to this effect. On the retention of data relating to electronic communications in the event of a serious, current or foreseeable threat to national security Article 11 quinquies provides that in the event of a serious threat, current or foreseeable, for national security, the Prime Minister may order electronic communications operators to retain, for a period of one year, certain categories of data relating to electronic communications, in addition to those mentioned in II bis. The bill also specifies that the Prime Minister's injunction, which takes the form of a decree whose duration of application cannot exceed one year, can be renewed if the conditions provided for its issuance continue to be met. . In this respect, the Commission recalls that the National Commission for the Control of Intelligence Techniques (CNCTR) is competent with regard to the implementation of intelligence techniques and is therefore one of the links in the operational chain leading to the collection of information. Consequently, it considers, insofar as the very principle of the retention of traffic and location data constitutes an invasion of privacy, that the Prime Minister's injunction requiring operators to retain this data should be subject to notice to the CNCTR. The Commission points out that such a procedure is particularly likely to guarantee a strict balance between the invasion of privacy caused by this collection and the protection of national security. In this respect, the Commission recalls that the European judge has made the generalized and undifferentiated collection of traffic and location data on the sole assumption of a serious threat to national security which proves to be real and current or foreseeable, this collection also having to be limited in time. In this context, the Council of State considered that the duration of this preservation injunction issued to operators could not reasonably exceed one year. The Commission considers that Article 11 quinquies, in that it provides that the duration of application of this injunction may not exceed one year, aims to meet the requirements set by the Council of State.On the conservation and access to data relating to electronic communications for the purpose of researching, establishing and prosecuting criminal offenses the retention of certain categories of data, for the purposes in particular of researching, recording and prosecuting criminal offenses in particular. of the decision of the Council of State of April 21, 2021. The Council of State ordered the Prime Minister to rescind his decision refusing to repeal article R. 10-13 of the CPCE as well as the decree from

February 25, 2011, in particular in that these provisions do not limit the purposes of the generalized and undifferentiated retention obligation of traffic and location data to safeguarding national security. This censorship is justified by the fact that the CJEU ruled that the general retention of this data for the purposes of the prosecution of criminal offenses was contrary to European Union law. However, the high administrative court considered that the criteria laid down by the CJEU to allow storage of these data for this purpose (targeted storage, predetermination of the persons likely to be involved in a criminal offence) were not materially feasible. On the other hand, it considered that so-called rapid retention of data to prevent the disappearance of information necessary for criminal investigations was permitted by European law. In concrete terms, it considered that this so-called rapid retention could result in an injunction from the judicial authority, issued to electronic communications operators, internet access providers and website hosts, to proceed with the retention (for a period of ninety days maximum) of the connection data they hold, including among those kept under the conservation imposed for the purposes of safeguarding national security. It is on this rapid storage that is added the possibility for the judicial authorities to access this data for criminal investigations relating to proven or suspected cases of serious crime. In this respect, the Commission understands the system as it submitted to it by the Ministry, that access to data, in particular traffic and location data, may be made possible by means of judicial requisitions. It recalls that the Council of State has made the possibility for the judicial authority to access the data necessary for the prosecution and investigation of the perpetrators of criminal offences, those whose seriousness justifies it. If in this respect, the preliminary article of the Code of Criminal Procedure (CPP) provides that the coercive measures to which the suspected or accused person may be subject are taken by decision or under the effective control of the judicial authority and that "they must be strictly limited to the requirements of the procedure, proportionate to the seriousness of the alleged offense and must not offend the dignity of the person", the Commission recalls, in any case, that a strict control of the he application of these provisions, given the invasion of the privacy of the persons concerned resulting from the retention of this data, will have to be carried out, both by the investigation services and by the judicial authorities. The Commission further notes that the bill, in that it modifies article L. 34-1 of the CPCE and article 6 of the law for confidence in the digital economy, leads to no specific provision governing now access to these d data for the purposes of research, observation and prosecution of criminal offences. Therefore, it wonders, given the specificity of the data to which it may be accessed, and in order to ensure the strict proportionality of this use, on the sufficiency of the current provisions, in particular with regard to the scope of application of Article 60-2 of the Code of Criminal Procedure, to regulate the methods of

so-called rapid retention of these data as well as their access (for example to set the maximum duration of rapid retention). In any case, the Commission emphasizes that, insofar as only offenses considered serious can justify such access, and as the public rapporteur underlined in his conclusions, fines should, in principle, be excluded from this perimeter.On the modification of the provisions relating to the obligations imposed on access providersThe draft law amends article 6 of law no. providers of access to online public communication services, retain identification data under the same conditions as those provided for in Article L. 34-1 of the CPCE. Subject to the reservations previously formulated, the Commission considers that the modification of this article does not call for any additional comments.On the prior control of the implementation of intelligence techniques (article 11 sexies of the bill)The bill amends the provisions provisions of Article L. 821-1 of the Internal Security Code (CSI) in order to provide that for all intelligence techniques, their implementation, in the event of an unfavorable opinion from the CNCTR, necessarily involves a referral to the specialized training of the Council of State by the CNCTR. In this case, the Council of State has twenty-four hours to rule, a period during which the intelligence technique in question cannot be implemented, except in the event of a duly justified emergency and if the Prime Minister Minister ordered its immediate implementation. In this respect, the Commission notes that these provisions aim to take into account the observations made by the Council of State in its decision of 21 April mentioned above, enlightened by the European requirements recalled by the CJEU. The implementation of all of these techniques is subject to a decision with binding effect, taken by a court or an independent administrative entity. The reform therefore amounts to submitting the implementation of an intelligence technique, except in an emergency, to the assent of the CNCTR, unless a court decision decides otherwise. The Commission welcomes the principle of such a development. It considers, however, that the draft law calls for the following observations. Firstly, the Commission considers that the mechanism is unnecessarily complex in that, instead of providing for an assent of the CNCTR, it provides for a referral to the Council of State, by members of the CNCTR and not the Prime Minister, in the event that an unfavorable opinion is issued. It also notes that the planned provisions formally allow the Prime Minister to authorize the immediate implementation of an intelligence technique after the unfavorable opinion of the CNCTR and before the Council of State has ruled. The Commission invites the Government to provide a simpler and more protective mechanism by providing for an assent from the CNCTR. It therefore recommends that, except in certain emergency cases, the Prime Minister be prohibited from authorizing the implementation of an intelligence technique after an unfavorable opinion from the CNCTR. It would then be up to the Prime Minister either to abandon the implementation of the technique, or to seize the Council of State himself.

Secondly, if the Commission understands that it is necessary, in view of the issues, that the formation of the Council of State rules as soon as possible, it considers possible that a period of twenty-four hours is not always sufficient to judge the most complex cases. In the event that the judge does not manage, despite his diligence, to settle the dispute within this period, it considers that it follows from the text that the intelligence measure cannot be implemented until it has not been authorized by the court decision.Thirdly, the bill repeals article L. 821-5 of the CSI which provides that in certain emergency situations and for limited purposes, the Prime Minister may authorize the implementation of an information technique without the prior opinion of the CNCTR. The Commission notes that the provisions introduced by the bill constitute a positive development insofar as the opinion of the CNCTR will be systematically requested, without possible derogation. It nevertheless emphasizes that in the event that the CNCTR issues an unfavorable opinion, the Prime Minister may, in the event of a duly justified emergency, order the immediate implementation of the technique, and this, before the Council of State be pronounced. However, the bill provides for limitations to this hypothesis, which can only be used for certain purposes (national independence, territorial integrity and national defence, the prevention of terrorism, and attacks on the republican form of the institutions, in accordance with article L. 811-3 of the CSI) concerning the sound system of certain places and vehicles as well as the capture of images and computer data. In addition, the nature of urgency cannot be invoked with regard to the so-called algorithm technique governed by Article L. 851-3 of the CSI. The Commission considers that this framework constitutes an important guarantee to ensure that the situations in which the emergency can be mobilized are limited to precisely defined cases. It nevertheless notes that for the majority of the intelligence techniques supervised by the CSI, the bill does not provide for any particular limitation as to the conditions under which the emergency could be mobilised. In this regard, the Commission considers that consideration could be given to the advisability of limiting the use of this emergency procedure to certain purposes considered to be the most serious, and this for all intelligence techniques. the transmission of information by the judicial authority to the intelligence services and to the National Information Systems Security Agency (article 11 septies)Article 11 septies of the bill regulates, for certain investigation procedures or investigation 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, as well as to the Agency National Information Systems Security Authority (ANSSI) of the elements of any kind appearing in these procedures and necessary for the exercise of their missions. 2 021-045 of April 15, 2021 relating to certain articles of the bill relating to the prevention of acts of terrorism and to intelligence, on provisions of a similar nature. In this

context, the observations developed below relate mainly to the changes envisaged by the Ministry, without prejudice to the remarks made in the aforementioned deliberation. the only IT and Liberties considerations, it nevertheless emphasizes that 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 such data, and more specifically those relating to the proportionality and legality of the processing. Firstly, the Commission notes that the scope of the offenses targeted by the draft law, although it is limited to cases which are or would appear to be very complex, nevertheless seems broad fact of some of the criminal offenses to which reference is made (for example with regard to the offenses of drug trafficking reliable), without the use cases corresponding to such a possibility being specifically identified and brought to its attention at this stage. Therefore, as formulated in its aforementioned deliberation, the Commission is wondering about the scope specifically targeted by Article 11 septies of the bill. Secondly, the bill provides that this information may, in this new version of the project, be transmitted to the so-called first and second circle intelligence services, for the sole missions relating to the prevention of crime and organized delinquency. In this respect, the Commission wonders about the reasons that led the Ministry to extend this possibility to the so-called second circle services. Thirdly, the draft law specifies that this communication may take place on the initiative of the public prosecutor or the investigating judge, or at the request of the intelligence services. In this respect, if the draft text specifies that in the context of a judicial investigation, this communication can only take place with the favorable opinion of the investigating judge, the Commission considers that the draft law should be clarified in order to expressly mention the optional nature, for the judicial authorities , of the transmission of such data, indicating that it is up to the judicial authority to assess whether this is likely to harm the proper administration of justice. President Marie-Laure DENIS