Deliberation 2021-040 of April 8, 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. 2021-040 of April 8, 2021 providing an opinion on a draft law relating to the prevention of acts of terrorism and intelligence (request for opinion no. 21005550) The National Commission for Information Technology and Liberties,Request by the Ministry of the Interior of a request for an opinion concerning a bill 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 by Mrs. Sophie LAMBREMON, Commissioner, and the observations of Mr. Benjamin TOUZANNE, Government Commissioner, Issues the following opinion Law No. 2015-912 of July 24, 2015 was intended to establish the legal framework applicable to the activities services of e intelligence by determining in particular the principles and purposes of public policy in this area, the legal regime applicable to intelligence techniques as well as the various guarantees that effectively allow them to be used. The CNIL is seized of a bill relating to the prevention of acts of terrorism and intelligence. This opinion does not comment on Articles 13 bis and 13 ter of the bill, introduced by an amending referral on which the Commission will rule later. The preservation of a strict balance between public security, the protection of fundamental interests of the Nation and respect for privacy led, by the 2015 law, to entrust the control of the various intelligence techniques to a specialized independent administrative authority (the National Commission for the Control of Intelligence Techniques or CNCTR) as well as to a specialized administrative court subject to cassation review by the Council of State. provisions relating to intelligence introduced in particular by law n° 2017-1510 of October 30, 2017 strengthening security internal affairs and the fight against terrorism (SILT law). In particular, it is a question of extending the nature of the data that can be collected in the context of access to connection data, as well as the possibility of transmitting information relating to a person subject to hospitalization. without consent, in particular to intelligence services, or to allow intelligence services to use data collected via intelligence techniques for purposes other than those that justified their collection, and to transmit this information to other services with intelligence duties. Given the challenges associated with the implementation of certain means considered to be particularly intrusive and making it possible to collect a very large volume of data, the Commission considers it essential to ensure that the breaches of respect for privacy are limited to the strict necessary. It recalls that these attacks must be adequate and proportionate to the aim pursued and that sufficient safeguards must be implemented. In this regard, the Commission observes that several of the guarantees introduced by the aforementioned law of 24 July 2015 are taken up by this draft law, such as the

strict formalism attached to the implementation of these techniques. The Commission notes that certain provisions of the bill are intended to provide a framework for the principles governing the collection of personal data, and therefore concern, and for the provisions relating thereto, data protection. It is for this reason that the Commission was seized, on the basis of Article 8-4°-a) of the law of January 6, 1978, with this draft law. The Commission recalls that the draft law regulates the methods of collection of the various information techniques provided for by the text. The data must then be processed, within various files implemented by the departments concerned, in compliance with the right to the protection of personal data, in particular Title IV of the Data Protection Act. However, the Commission recalls that most of them (listed in Decree No. 2007-914 of May 15, 2007) benefit from a derogatory regime, which allows them to be excluded from the scope of the Commission's a posteriori control, in accordance with article 19-IV of the amended law of 6 January 1978. With regard to the planned developments, both in terms of the data collected and the use and transmission of this information, the Commission recalls, as it has done in the past, that it asks to be able to exercise its powers of control over this processing. While it notes that both the CNCTR (through its opinion on the implementation of techniques, as well as its monitoring of the execution of authorizations granted by the Prime Minister) and the interministerial control group (GIC) have prerogatives aimed in particular at ensure the legality of the practices implemented, the Commission considers that its control, which would relate to the overall conditions of implementation of the said files and should be accompanied by guarantees adapted to their particular nature, should supplement those already carried out by these two entities and would constitute an additional guarantee.Finally, the Commission notes that the Court of Justice of the European Union ruled on October 6, 2020 (Privacy international (case C-623/17), and La Quadrature du Net, French Data Network , Ordre des barreaux francophones et germanophone (joined cases C-511/18, C-512/18, C-520-18)), in the context of a preliminary question, on the conformity of certain of the provisions referred to by the bill. If it does not intend to assess, in its opinion, the regularity of the provisions already in force and not modified by the draft with regard to European Union law, for which the Government has indicated that it is waiting for the outcome of the ongoing litigation, the Commission nevertheless recalls that the European judge ruled on the conditions of lawfulness for the implementation of intelligence techniques for real-time collection and automated analysis of traffic data and technical data relating to the location of equipment. However, several provisions of the bill examined relate to these techniques. The European judge admitted the use of these methods for the purpose of combating terrorism. The guarantees required by the European judge relate in particular to the existence of a serious threat to national security which proves to be

real and current or foreseeable and which justifies the surveillance, and to the existence of an effective control of the processing algorithmic screening, either by a court or by an independent administrative entity whose decision has binding effect. In this respect, the Commission notes that French legislation has established an independent administrative authority, the CNCTR, which is called upon for advice on any authorization to implement these intelligence techniques, has powers of control over their implementation, may address to the Prime Minister any recommendation deemed necessary and may seize, when its opinions or recommendations are not acted upon, a specialized court whose decision is binding on the intelligence services. On the other hand, if article L. 801 -1 of the internal security code provides that the authorization of these techniques must be justified by the threats, risks and issues related to the fundamental interests of the Nation, the Commission recommends that the drafting of the bill make explicit that it falls within the office of the CNCTR to verify the existence of this threat of a terrorist nature. Such a control, recalls the CJEU, must indeed be carried out when deciding to proceed with the processing of automated analysis of connection data, or when renewing its authorization. The Commission notes that, with regard to the real-time collection of the connection data of certain persons, the Court has required that it be limited to persons for whom there is a valid reason to suspect that they are involved in a way or another in terrorist activities, which should be clarified. Finally, the Court also insisted on the need to provide appropriate, general and sometimes individual information on these measures, without undermining their effectiveness. The law or the regulatory provisions will have to incorporate these requirements. Given the strong impact that Parliament's choices could have on the implementation of certain intelligence techniques, the Commission points out that it will be particularly vigilant with regard to the developments that could be made to the devices in question (and in particular the measures of necessity and proportionality which will be required in any event). It stresses in any event that it must be consulted on aspects falling within its competence. algorithm (articles 1, 7 and 8 of the bill) Article L. 851-3 of the Internal Security Code (CSI) in its wording resulting from the aforementioned 2015 law provides for the possibility of implementing on the networks of electronic communication of operators and certain other legal persons, automated processing intended to detect, by means of an algorithm, connections likely to reveal a terrorist threat.As a preliminary point, the Commission notes the difference between the characteristics of the first processing implemented in 2017, which related only to telephony, and those of those envisaged in application of the same text which, due to the evolution of practices in this area as well as the type of information concerned, raise specific issues. It notes in this regard that Article L. 851-3 of the CSI governs both the processing of telephone data and data from Internet connections. In this respect, the

Commission stresses that the experiment whose continuation is planned relates to these two types of data, indiscriminately, even though its implementation has so far only related to data of telephony. It considers that the invasion of privacy by the algorithmic screening of connection data on the Internet is however greater than that of telephone connection data and that the proportionality check must be differentiated. implementation of this technique Article 8 of the draft law provides that these algorithms may be authorized, at the request of the specialized intelligence services mentioned in Article L. 811-2, on data passing through the networks of operators and of the persons mentioned in Article L. 851-1 (…). It also specifies that only one service of the Prime Minister is authorized to carry out the processing and operations implemented on the basis of I and IV, under the control of the National Commission for the Control of Intelligence Techniques. The ministry specified that the modality initially envisaged to implement this technique, consisted in physically placing the detection devices at several points of the networks of the operators. The Commission notes that this method corresponded to the most natural interpretation of Article L. 851-3 of the CSI, resulting from the 2015 law and would have constituted a form of technical guarantee provided to the device. The Ministry nevertheless indicated that physically placing the detection devices at several points of the networks of the operators presents technical difficulties, both in terms of security of the networks of the operators, and of detection of events common to several devices installed on these networks. In addition, as some of the detection parameters are particularly sensitive, they cannot be made accessible or divulged during the execution of the algorithm by the operators. Consequently, the Ministry has adopted an architecture according to which the data flows are not analyzed by means of algorithms installed on the networks of the operators but duplicated then routed within an infrastructure dependent on the State to be subjected to centralized detection devices. The CNCTR has given its agreement to these technical methods, which it considers to be in conformity with the law authorizing experimentation, by requiring certain guarantees, in particular the fact that the algorithm is implemented by the GIC and not by the services of information. With regard to these procedures, the Commission makes the following observations, given the information made available to it. The Commission considers that the amendments made by the draft law to Article L. 851-3 of the CSI do not make it possible to understand in a clear and precise manner the changes envisaged and thus the way in which this intelligence technique will be implemented. It considers it essential that the text be clarified. It considers in particular that the fact that the implementation of the algorithm involves duplicating, for the benefit of an administrative department of the Prime Minister, all of this data, which concerns all telephone calls and internet access made in the territory French, is a particularly significant development. Centralization and duplication

modify the scope of the invasion of privacy, by the risks they carry in themselves. The very principle of this technical architecture should therefore, in its view, be included in the law. The Commission considers, a fortiori, that specific guarantees, provided for by the texts, must necessarily surround the implementation of such a technical architecture. These guarantees must ensure that the provision of all of this data to the GIC, apart from any targeted surveillance measure, cannot be analyzed as a form of real-time collection of connection data, which would be prohibited by European case law. In this respect, if the connection data themselves are not made available to the intelligence services and can only, under the control of the CNCTR, be used by the GIC for the implementation of the algorithm, the Commission considers that it is also necessary that the data be kept only for the time strictly necessary for their analysis, then immediately destroyed, and that the GIC only keep the strict minimum necessary for the operation of the algorithm over the period of analysis considered. In this respect, it takes note of the clarifications provided by the Ministry according to which these data are kept in pseudonymous form for a period of twenty-four hours (except in the event of a hit), before being destroyed. This clarification should be expressly included in the bill, which should also specify the procedures for collecting and accessing this data. Regarding the use of an algorithm The use of this very specific intelligence technique, according to the procedures described above, can only be accepted if it is necessary and proportionate to the objective of combating terrorism. intelligence of adequate means of action in the face of persistent threats that weigh on the fundamental interests of the Nation and, more particularly, to allow the early detection of terrorist threats. The Government considers that this new intelligence technique is made necessary by the evolution of the terrorist threat, which would come from individuals who do not belong to structured and identifiable groups or organizations, whose radicalization and taking action are poorly apprehended by targeted intelligence techniques. The Government has also emphasized that these algorithmic processing operations are used to identify people whose intelligence services then determine, under the control of the CNCTR, whether it is necessary to subject them to a targeted surveillance measure in the event of a suspected terrorist threat. This balance responds to a requirement of the CJEU which requires that the use of the algorithm does not lead to an automated decision of targeted surveillance. The processing of all the connection data with the actors concerned makes it possible to detect individuals whose radicalization could be detected by their digital activity, in particular by means of a hit/no hit mechanism, in order to subsequently trigger targeted surveillance.Finally, the implementation of this technique is surrounded by a series of guarantees and controls, consisting in particular in making the implementation of such a technique subject to an authorization from the Prime Minister after consulting the CNCTR, the latter

having a power of recommendation and referral to a specialized court whose decisions are binding. In addition, the Government provides in the bill that this technique can no longer be exercised directly by the intelligence services but by a separate service of the Prime Minister (the GIC), under the control of the CNCTR. The bill also proposes removing the possibility of extending the retention period for data resulting from this technique. On the other hand, the Commission can only point out that the use of such a technique is particularly strong privacy of individuals and the right to the protection of personal data, guaranteed in particular by the Constitution and the Charter of Fundamental Rights of the European Union, since it is not of a targeted nature but proceeds from the analysis of the set of population connection data. The implementation of extensive monitoring of all connection data could, on its own, have chilling effects on the exercise of their freedom of information and expression by Internet and network users. of electronic communications. In addition, the specific methods of implementing these algorithms accentuate the breach of respect for the privacy of individuals and the protection of their personal data. recalls that the processing implemented by means of algorithmic processing consisting of analyzing connection and location data constitutes processing of personal data. In the aforementioned decision of the CJEU, it was recalled that the information referred to (traffic and location data) provide the means to establish the profile of the persons concerned insofar as they relate to a significant number of aspects of the privacy of data subjects, including sensitive information (…). In this respect, the Commission considers that the wording of Article L. 851-3 of the CSI, which mentions that the data concerned are collected without allowing the identification of the persons to whom the information relates, should be modified insofar as these data are likely to allow the identification of persons. The Commission observes in particular that this automatic tracking technique is likely to lead to the collection and analysis of connection data of any person, including those whose communications are subject to , according to national rules, to professional secrecy.Finally, the Commission recalls the risk linked to the inclusion of bias in the algorithms deployed, during the design or training of the models, which can lead to false positives or false negatives affecting in particular the operational efficiency of the system and leading to harmful consequences for the persons concerned. The Commission considers that the Ministry should initiate work on the subject and recalls the need to be particularly vigilant in the context of these different phases of development of algorithmic models. The Commission also takes note of the clarifications of the Ministry which indicated that the algorithms are based in principle on models generating the hit/no hit signals from strict selectors, often coming from traditional intelligence methods. This solution not only contributes to the operational efficiency of the intelligence measure but also constitutes a more protective solution for privacy and contributes to

ensuring the proportionality of the system. It therefore encourages the Ministry to build a usage doctrine that favors this type of algorithm. As a result of the above, the Commission considers that the introduction of such surveillance techniques into French law can only be justified under very strict conditions. It notes that the bill maintains the limitation of this technique to the sole purpose of detecting terrorist threats. It was necessary to proceed by experimentation, as the 2015 law did, and the sustainability of this technique is only possible if, on the one hand, the protection of the population against terrorist threats cannot be ensured by satisfactorily by the traditional means of targeted surveillance, which it is up to the Government to establish, and if, on the other hand, this technique is accompanied by sufficient guarantees to limit its use to what is strictly necessary and to ensure that abuses are identified and penalized. With regard to the principle of sustainability Article 1 of the bill provides for the sustainability of the implementation of the so-called algorithm intelligence technique, hitherto experimental and expiring on December 31, 2021 The guarantees provided are mainly those previously presented. the years of experimentation, to compare them to the invasion of privacy represented by this very particular form of surveillance. In this respect, the law requires the Government to submit a report on the application of this provision to Parliament by 30 June 2021 at the latest. The Commission has taken note of a general assessment of the experiment but considers that the Ministry did not provide it with sufficiently precise elements allowing it to assess the operational effectiveness and efficiency of this technique (such as a report including quantitative elements on the number of cases identified, false positives, lifting of pseudonyms , duration of use of these algorithms, etc.). It was indicated that elements protected by national defense secrecy would be provided to other authorities, in particular the parliamentary intelligence delegation. Under these conditions, it considers that it is not in a position to assess the benefits of this intelligence technique and, consequently, to assess the proportionality of the breach it causes to respect for private life. of data relating to complete addresses of resources on the Internet (sections 8 and 9 of the bill) Sections 8 and 9 of the bill provide for additional information that may be subject to automated collection and monitoring complete addresses of resources on the Internet . This modification applies to the two techniques of administrative data collection, namely real-time data collection and collection by means of algorithmic processing (provided for respectively in Articles L. 851-2 and L. 851-3 of the CSI) . As a preliminary point, the Commission considers that the concept of complete addresses of resources on the Internet, added to articles L. 851-2 and L. 851-3 of the CSI is not strictly identical to the concept of URL, often used in the documents sent by the ministry as part of the examination of the request for an opinion. Indeed, if the URL mechanism can be used to designate resources stored on a server, many services also use it to transmit information to a

server or to store elements relating to the current session. This is the case, for example, with query strings request parameters and information from HTML forms filled out by users, this data being aggregated at the end of the URLs and transmitted with them. It therefore invites the government to consider the precise scope it intends to define and to refine the formula. If the experiment were to concern all URLs, a formula of the resource address type on the internet and parameters associated with this address could be considered. a URL consulted by an Internet user by obtaining the details of the DNS resolutions that he would have carried out with his Internet access provider, it is different for the full path of the resource. Indeed, the URL cannot be read in plain text by the operator when the transmission of data concerned is encrypted between the user's terminal and the servers concerned (via the HTTPS protocol for example, which is used today today for almost all connections on the web). The Commission notes that the collection from operators only targets unencrypted URLs, decryption not being envisaged by the intelligence services at this stage. As regards the admissibility of the extension of these two intelligence techniques to URLs, the Commission recalls that these data have a specific nature. As pointed out by the European Data Protection Board (EDPS), URLs are likely to reveal information relating to the content of the items consulted or correspondence exchanged. The Commission recalls that the special protection enjoyed by content data and correspondence represents an essential guarantee to ensure respect for privacy and other related freedoms. The Constitutional Council, in its decision n°2015-713 DC of July 23, 2015 concerning the law relating to information, noted (pt 55), under the guarantees applied to the collection or processing methods in question, the impossibility of collecting data relating to the content of correspondence exchanged or information consulted, in any form whatsoever, within the framework of these communications. It is in particular with regard to this guarantee and, in accordance with the analysis of the Government, which had then specified that the device of the algorithms would relate only to connection data (or metadata) and not to the content of the communications, that he declared the aforementioned intelligence techniques to be compliant. whose communication techniques such as the terrorist threat are changing rapidly, considers that it is not possible for it to comment on the proportionality of such an attack ex ante. It therefore considers that, as for the principle of the technique of surveillance by algorithmic processing, the legislator should initially, and including if it chose to perpetuate the technique of algorithmic intelligence, pass again, on this point, by an experiment before extending it definitively to these new categories of data. This experiment could make it possible, more generally, to assess in detail the usefulness of this intelligence technique for all connection data linked to the use of the Internet since, according to the Commission's understanding, the only algorithms used so far were for telephone connection data. On the retention of data

for purposes of research and development of intelligence techniques (article 11 of the bill) Article 11 of the bill plans to complete the article L. 822-2 of the CSI in order to provide for the retention and reuse of data collected through intelligence techniques for the sole purposes of intelligence research and development. Storage for this purpose may not exceed five years after data collection. The Commission, which is deciding for the first time on such a provision, notes that the implementation of such a system is not intended to make it possible to track and/or identify people, in the same way as intelligence techniques, but to use this data for research purposes, to allow the development and improvement of the capacities of collection techniques and exploitation. It underlines that if the purposes of conservation and exploitation of this information, legitimate, are quite distinct from those having justified their collection, the fact remains that the processing of this data, and in l The absence of any measure allowing the total anonymization of this information constitutes a processing of personal data within the meaning of the applicable regulations. In this respect, and taking into account the purposes for which such processing would be implemented, the Commission considers that the amended law of 6 January 1978, and more particularly its title IV, is intended to apply to the planned processing, under subject to special provisions of the CSI derogating therefrom. On this last point, it notes in particular that the research programs would not have to be authorized by regulatory acts pursuant to Articles 31 et seq. of the law of 6 January 1978 since the draft law already provides for a mechanism specific authorization. It recalls that, with regard to the aforementioned law, its article 4-2° provides that the subsequent processing of data for research purposes is considered to be compatible with the initial purposes of the data collection, s it is carried out in compliance with the applicable data protection provisions. The Commission notes that the Ministry, in order to ensure, as provided for in the bill, that this storage is carried out to the extent strictly necessary for sufficient knowledge to develop, improve and validate the technical capacities of data collection and exploitation has accompanied the implementation of this system with guarantees. In this respect, only agents specially authorized for this purpose and exclusively assigned to this mission will be able to access the data, the reasons and purposes for which the information was collected will not be kept, and finally, it will not be possible to search for the identity of a person through this device. The technical parameters of each research program will be authorized by the Prime Minister, after consulting the CNCTR, which will be able to use its powers of control, recommendation and referral to the judge. The Commission welcomes the implementation of these guarantees. It nevertheless considers that the data reuse regime, as a whole, should be governed by an implementing decree and that additional guarantees should be provided in the event that this processing is implemented by means of algorithmic processing. Indeed, the methods as well as the criteria

taken into account by the algorithmic processing must be clearly defined before any implementation of the planned processing and particular attention must be paid to the cardinal principles of vigilance and loyalty throughout the development of this treatment. On the one hand, given the particular sensitivity of the information likely to be processed as well as the volume of data intended to be used, particular attention will have to be paid to the planned developments in algorithmic processing and more particularly to the presence of possible biases. It also calls for vigilance on the processing of any sensitive data when training algorithms. On the communication of information relating to the admission of a person subject to a hospitalization measure without consent (article 6 of the bill)Article 6 of the bill provides for the introduction of an article L. 3211-12-7 to the public health code in order to allow the communication of information relating to the admission of a person in psychiatric care without consent, to the representative of the State in the department, and in Paris, to the prefect of police, as well as to the intelligence services mentioned in articles L. 811-2 and L. 811-4 of the CSI in order to ensure the follow-up of this person who represents a serious threat to security and public order because of his terrorist radicalization. Such information is now only communicated to the prefect of the hospitalization department of the person concerned. hospitalization of the person concerned. Although the principle of derogation from medical secrecy is covered by law, the Commission recalls that the conditions for implementing this possibility must be strictly regulated by regulation (and in particular the provisions relating to the files concerned). In this respect, the Ministry plans to implement this possibility by means of a connection between the File for processing reports for the prevention of terrorist radicalization (FSPRT) and the processing of personal data relating to the follow-up of people in psychiatric care without consent called HOPSYWEB. In the event that the provisions introduced by the bill would only be intended to allow such a possibility, and thus be limited to the only linking between these two files, the Commission recalls the observations made in its deliberation No. 2018- 354 of December 13, 2018 in which, without calling into question the legitimacy of such transmission, it had strongly questioned the conditions for its implementation. More particularly, and with regard to the particular sensitivity of information relating to a admission to psychiatric care covered by medical secrecy and at the risk for the persons concerned, it calls for strict supervision of the conditions for implementing this transmission, in particular strengthening the security of procedures for verifying identity and collecting 'further information. The Commission also recalls that the information communicated must be strictly necessary for the performance of the missions of the representative of the State and the intelligence services and be limited to what is provided for in Articles L. 3212-5, L. 3212- 8 and L. 3213-9 of the Public Health Code and Article 706-135 of the Code of Criminal Procedure. On the transmission

of information covered by secrecy protected by law to the intelligence services (Article 10 of the draft of law)The amendments to article L. 863-2 of the CSI by article 10 of the bill aim to authorize the administrative authorities mentioned in article 1 of ordinance no. 2005-1516 of December 8, 2005 relating to electronic exchanges between users and administrative authorities and between administrative authorities, to be transmitted to the information services mentioned in Articles L. 811-2 and L. 811-4 of the CSI, on their own initiative or at the request of the latter , any information m even covered by a secret protected by law, strictly necessary for the accomplishment of the missions of these services and likely to contribute to the defense and promotion of the fundamental interests of the Nation mentioned in article L. 811-3 of the same code . These provisions modify the current article L. 863-2 of the CSI which authorizes these transmissions when they are only useful for the missions of these services. essential to the intelligence services to enable them to carry out their missions and welcomes the tightening of the conditions laid down by law. some of them. She considers that the text does not cover the hypothesis of a medical professional practicing in a public structure. The Commission recalls that the conditions for implementing such transfers must be specified and framed by regulation, as already provided for in Article L. 863-2 of the CSI. It particularly insists on the vigilance that must be brought to the transmission of information carried out on the initiative of the administrative authorities, as well as to the guarantees surrounding the exemptions from medical secrecy. In any event, the Commission considers that Article L. 863-2 of the CSI should be amended in order to guarantee that such attacks can only be necessary and proportionate to the interests pursued. On exploitation for other purposes , information collected through intelligence techniques, and their transmission to other intelligence services (article 10 of the bill)Article 10 of the bill provides that when a specialized intelligence service mentioned in article L. 811-2 or a service designated by the Conseil d'Etat decree provided for in Article L. 811-4 obtains, following the implementation of a technique mentioned in Title V of this book, useful information for the pursuit of a purpose different from that which justified the collection, he can transcribe or extract them for the sole exercise of his missions. This article also provides that, subject to the provisions of the second to fourth paragraphs of this II, a specialized intelligence service mentioned in article L. 811-2 or a service designated by the Conseil d'Etat decree provided for in l Article L. 811-4 may transmit to another of these services the information collected, extracted or transcribed at its disposal, if this transmission is strictly necessary for the performance of the missions of the recipient service. As a preliminary point, the Commission notes that the draft law aims to provide a stricter framework than in the current article L. 863-2 of the CSI, the methods according to which the data collected via intelligence techniques may be used and transmitted to other services carrying out intelligence

missions. It emphasizes that strong guarantees are also provided for by the text, under which there is prior authorization from the Prime Minister after consulting the CNCTR for some of these transmissions, as well as the appointment of an agent, within each specialized service. intelligence, responsible for ensuring compliance with the application of the aforementioned provisions. These safeguards are such as to ensure a fair balance between the possibility of using this information for intelligence purposes and the protection of the data thus concerned. The Commission recalls first of all that Article L. 811-3 of the CSI limits the purposes that may justify the use of an intelligence technique, and also recalls that article 4-2° of the law of January 6, 1978 provides that personal data must be collected for specified, explicit and legitimate purposes, and not to be further processed in a manner incompatible with those purposes. The Commission insists on the fact that the information may only be transmitted to another service for the performance of the tasks defined by its constituent texts. These missions are, for the so-called inner circle intelligence services, exhaustively listed in Article L. 811-3 of the CSI. It emphasizes that it will be up to the CNCTR to ensure, on a case-by-case basis, that the subsequent use of information obtained by particularly intrusive techniques, in principle prohibited to administrations, is not disproportionate with regard to the usefulness of the information for the service to which it is addressed and the objectives pursued. This control is particularly necessary when the information will be transmitted to one of the so-called second circle services, provided for in Article L. 811-4 of the CSI, for a mission not falling within the purposes listed in Article L. 811-3 of the same code. It would like the bill to mention this compatibility check incumbent on the transmitting service and the CNCTR. In addition, if the Commission notes that the information transmitted to the intelligence services of the second circle will necessarily be transmitted with regard to one of the purposes mentioned in Article L. 811-3 of the CSI and provided that it corresponds to the missions entrusted by regulation to the service to which it is addressed, it considers that the text is ambiguous on this point and should be clarified. developments likely to have an impact on the regulations relating to the protection of personal data or which, at the very least, could be analyzed with regard to the principles set by the law of January 6, 1978 as amended. In general, if the Commission considers that these various amendments do not call for any substantial comment; it nevertheless raises the following points.Article 4 of the draft law aims to allow the seizure of a computer medium present at the scene of a home visit ordered for the purposes of preventing the commission of acts of terrorism, when this has revealed elements related to the threat and that the person obstructs access to the computer data it contains. The Commission notes that the entry and processing of this data will be carried out under the same conditions as those currently provided for by Article L. 229-5 of the CSI, which does not call for comment. Article 10 of

the bill modifies article 49 of the law of January 6, 1978 in order to provide that the right of access of the persons concerned does not apply with regard to the information according to which personal data have been transmitted in application of the first paragraph of article L. 863-2 of the CSI. The Commission recalls that Article 23 of the aforementioned GDPR provides that the law of the Member State may, by legislative means, limit the scope of the rights of data subjects, where such a limitation respects the essence of the fundamental rights and freedoms and that it constitutes a necessary and proportionate measure in a democratic society, in particular to guarantee national security and defence. Thus the duration of authorization of the technique of collecting computer data is aligned with that of capture. Finally, article 14 modifies article L. 213-2 of the heritage code to clarify the system of communicability of classified archives .The PresidentMarie-Laure DENIS