Deliberation 2020-103 of October 15, 2020Commission Nationale de l'Informatique et des LibertésNature of the deliberation: OpinionLegal status: In force Date of publication on Légifrance: Tuesday November 23, 2021NOR: CNIX2131240VDeliberation n° 2020-103 of October 15, 2020 providing an opinion on a draft decree amending decree no. 2014-1162 of October 9, 2014 relating to the creation of the "National Platform for Judicial Interception" (PNIJ) and the Code of Criminal Procedure (second part: decrees in Council of State) (request for opinion no. 19022399)The National Commission for Computing and Liberties, Seizure by the Minister of Justice of a request for an opinion concerning a draft decree amending decree no. 2014-1162 of October 9 2014 relating to the creation of the National Platform for Judicial Interception (PNIJ) and the Code of Criminal Procedure (second part: decrees in the Council of State); Having regard to Convention No. 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data; Having regard to Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention and detection of crime criminal proceedings, investigation and prosecution in this area or the execution of criminal penalties, and on the free movement of such data and repealing Council Framework Decision 2008/977/JHA; Having regard to the Customs Code, in particular its article 67 bis-2; Having regard to the Code of Criminal Procedure, in particular Articles 230-45 and R. 40-42 to R. 40-56; Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its articles 32 and 89-II; Having regard to Law No. 2016-731 of 3 June 2016 strengthening the fight against organized crime, terrorism and their financing, and improving the efficiency and guarantees of criminal procedure; Having regard to Law No. 2019-222 of March 23, 2019 on programming 2018-2022 and reform for justice, in particular its article 47; Having regard to Decree No. 2017-614 of April 24, 2017 creating a service with national jurisdiction called the National Agency for Digital Judicial Investigation Techniques and a Steering Committee for Digital Judicial Investigation Techniques; Having regard to decree n° 2019-536 of May 29, 2019 as amended, taken for the application of law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms; Having regard to deliberation no. 2014-009 of January 16, 2014 providing an opinion on a draft decree authorizing the implementation of automated processing of personal data called the National Platform for Judicial Interception; Having regard to deliberation no. 2015-358 of October 15, 2015 providing an opinion on a draft decree in the Council of State amending decree no. 2014-1162 of October 9, 2014 creating an automated processing of personal data called Plate - national form of judicial interceptions; Having regard to deliberation no. 2016-383 of December 8, 2016 providing an

opinion on a draft decree amending decree no. 2014-1162 of October 9, 2014 relating to the creation of the National Platform for Judicial Interception; Having regard to deliberation no. 2017-343 of December 21, 2017 providing an opinion on a draft decree amending decree no. 2014-1162 of October 9, 2014 relating to the creation of the National Platform for Judicial Interception; MAUGÜÉ, commissioner in his report, and Mr. Benjamin TOUZANNE, government commissioner, in his observations,Issuing the following opinion: The draft decree submitted for opinion to the Commission aims to modify decree no. October 9, 2014 relating to the creation of the National Platform for Judicial Interception (PNIJ) and the Code of Criminal Procedure. The Commission observes that Article 230-45 of the Code of Criminal Procedure provides that a Conseil d'Etat decree, issued after a public and reasoned opinion from the National Commission for Computing and Liberties, determines the missions and operation of the national platform for judicial interception. The Commission notes that the PNIJ replaced the transmission system for judicial interception (STIJ) which had been authorized by Decree No. 2007-1145 of July 30, 2007 and which has ceased to operate since May 31, 2018. The purpose of the PNIJ, within the framework of the investigations and judicial information provided for by the CPP, is to centralize the data resulting from: the results of the interception of electronic communications and geolocation measurements; requisitions for the purpose of transmitting connection data kept by electronic communications operators, Internet access providers and hosts.The Commissio n notes, on the one hand, that the envisaged modifications aim to take into account legislative and regulatory developments which require a modification of the regulatory provisions of the Code of Criminal Procedure (CPP) relating to the PNIJ and which result from Laws No. 2016- 731 of June 3, 2016 and n° 2019-222 of March 23, 2019 mentioned above as well as decree n° 2017-614 of April 24, 2017 creating the national agency for digital judicial investigation techniques (ANTENJ) which was substituted for the delegation to judicial interceptions. Article 230-45 of the CPP has thus been introduced, which now makes the use of the PNIJ compulsory, unless technically impossible, for the implementation of article 709-1-3 of the CPP (use of a interception and/or geolocation in real time) and for the transmission of requisitions for the purposes of geolocation within the framework of Article 67 bis-2 of the Customs Code. The Commission observes, on the other hand, that the draft decree provides for the possibility that the PNIJ may be used optionally for the centralization and storage of data relating to public address measurements, and that it extends the list of recipients who may access to processing.On the general conditions for implementing the systemFirstly, the Commission recalls that it had considered, with regard to the extent of the data processed and the nature of the investigative acts concerned, that legal measures and appropriate techniques should be provided in order to ensure a high level of data

protection. the compliance of the processing with the regulations relating to the protection of personal data. It notes that this personality can order all the measures necessary for the exercise of its control but that it will not have access to the data recorded in the processing, as well as the members of the committee which assists it. The qualified person is also responsible for drawing up an annual report which he sends to the Keeper of the Seals, Minister of Justice. The Commission recalls that it had taken note of the ministry's commitment to send it this annual report and that it had indeed received this report in 2017. It asks to continue to receive it. Finally, it observes that it is provided in the draft decree that the powers entrusted to the qualified personality are exercised without prejudice to the control exercised by the Commission.Secondly, if the Commission notes that data relating to minors may be recorded in the processing, it acknowledges that the ANTENJ does not have access to the data, in order to guarantee their confidentiality, and will therefore not be able to identify the data relating to this category of persons in order to place specific measures. On the scope of the planned system The Commission observes that it follows from Article 230-45 of the CPP that recourse to the PNIJ is now made compulsory for requisitions and requests sent pursuant to Articles 60-2, 74-2, 77 -1-2, 80-4, 99-4, 100 to 100-7, 230-32 to 230-44, 706-95 and 709-1-3 of this code or article 67 bis-2 of the code Customs, unless technically impossible. The Commission notes that this draft decree also aims to expand the use of the PNIJ, on an optional basis, for the centralization and storage of data from public address measurements provided for in Articles 706 -96 to 706-99 of the CPP, these measures being reserved for certain types of serious offense listed in articles 706-73 and 706-73-1 of the CPP. In this context, the Commission notes that it is left, at the convenience of the investigator, the possibility of using the two service providers outside the PNIJ subsi stant […] particularly for French Polynesia where the PNIJ is not yet effective or in the event of a major temporary malfunction of the platform and that, in addition, there are sound measures that do not go through a SIM card, by example when a listening system is placed in a room and then raised. Therefore, a request for operations, through the PNIJ, is not necessary and these measures can therefore be processed outside the PNIJ. Without calling into question the legitimacy of such an extension, the Commission considers that the scope of the system will be substantially extended by allowing the use of the PNIJ for sound measurements. However, it notes that the purpose of this modification is to secure the storage and processing of data relating to sound measures as well as the traceability of accesses, which are currently carried out in a disparate manner. On the applicable legal regime and the purposes of the processing Draft article R. 40-43 of the CPP provides that, in order to facilitate the observation of offenses against criminal law and customs offences, the collection of evidence of these offenses and the search for their perpetrators or

to provide proof of the violation of certain prohibitions resulting from a conviction, the PNIJ makes it possible to make the data and information contained in the processing available to: magistrates, officers and judicial police officers of the national gendarmerie and police responsible for assisting them as well only customs officers and tax services authorized to carry out judicial investigations; agents authorized by the Minister responsible for customs to carry out customs investigations. Firstly, the PNIJ processing is implemented in particular for the purpose of facilitating the observation of offenses by gathering evidence of these offenses and allowing the search for their perpetrators or to bring evidence of violation of certain prohibitions resulting from a conviction. It makes it possible to transmit to electronic communications operators interception and geolocation requisitions as well as requests for connection data issued by magistrates, judicial police officers and agents of the national gendarmerie and police as well as agents of the judicial customs and tax services authorized to carry out judicial investigations, which can be qualified as a competent authority within the meaning of article 87 of the LIL. The Commission considers that it therefore falls within the scope of Directive (EU) 2016/680 of 27 April 2016 referred to above (hereinafter the Directive) and must be examined in the light of the provisions of Articles 87 et seq. law of 6 January 1978 as amended.Secondly, with regard to the purposes of the processing, the Commission notes that the draft decree makes it compulsory to use the PNIJ, in accordance with article 230-45 of the CPP, for requisitions and requests sent pursuant to Article 67 bis-2 of the Customs Code, unless technically impossible. The Commission notes that the customs offenses covered by this provision are those indicated in Article 67 bis-2 of the Customs Code which are punishable by a prison sentence of three years or more. , the Commission notes that the draft decree makes it possible to use, on an optional basis, the PNIJ for the centralization and storage of data resulting from the public address measures provided for by articles 706-96 to 706-98 of the CPP.Finally, the Commission notes that it appears from the details provided by the Ministry that if an additional purpose of the PNIJ was initially envisaged in order to allow the certification of legal costs related to electronic requisitions on the basis of Article R. 225 of the CPP , the Ministry finally made the choice to implement separate processing for this purpose and that the impact assessment relating to data protection (DPIA) will be updated on this point. The Commission considers that the intended purposes are determined, explicit and legitimate in accordance with article 4-2° of the law of January 6, 1978 as amended. The processing being likely to relate to data mentioned in I of article 6 of the law of January 6, 1978 modified, it must be authorized by decree in Council of State taken after reasoned opinion of the Commission in accordance with article 32 and with the II of article 89 of the law of January 6, 1978 modified. Without calling into question the legitimacy of the creation of

such processing, the Commission nevertheless considers, with regard to the extent of the processing and the conditions for its implementation, as well as the entry into force of the Police-Justice Directive as transposed, that the draft decree calls for various observations, in particular on the following points: safeguards aimed at specifically regulating the recording of so-called sensitive data must be implemented; the retention period for logging data, which has not been modified ed by the draft decree, does not appear to comply with the recommendations of the Commission; the procedures for exercising the rights of the persons concerned, in particular for the persons appearing in the PNIJ under a contact with the target person or under of a questioning following which no prosecution will be initiated, cannot be systematically refused and should be redefined.On the data collectedThe draft article R. 40-46 of the CPP lists the categories of data that may be recorded in the processing depending on the means of data collection used, namely: electronic communications subject to judicial interception; electronic communications subject to a geolocation measure in real time; the data and information communicated pursuant to Articles 60-2, 77-1-2, 99-4, 712-16, Articles R. 10-13 and R. 10-14 of the Post and Communications Code electronics and Decree No. 2 011-219 of February 25, 2011; the data, information and content of conversations obtained during a public address measurement; the real-time geolocation data obtained during a public address. It also takes note of the modification of the draft decree by the ministry in order to add, in 6° of article R. 40-46 of the CPP, a new category of data collected, those necessary for the use and security of the PNIJ for allow the collection of the identity of the natural person holding access to the PNIJ, as well as his ranks, functions and the identity and organization reference number (RIO) or the functional number, the designation of the service or the user's jurisdiction and the associated postal address, telephone and fax number, as well as the e-mail address. It is also specified in this provision that information relating to the voice recognition of the speaker. Firstly, the Commission notes that this draft decree does not provide for an automated device allowing a reconciliation between several cases. It also notes that the personal data collected may be relating to different categories of persons, namely the users of the PNIJ (investigators, magistrates, etc.) and the persons targeted by the measures and indirectly concerned, this last category grouping together the persons directly targeted by the measure (the requisition of data from connection or even interception) and the persons targeted only indirectly, such as the persons in contact with the person primarily targeted by the investigating services. It notes that, if different categories of people are affected by the processing, the data controller will not be able to distinguish the data of these different categories of people since the ANTENJ, for reasons of confidentiality, will not be able to access to data. Secondly, the Commission observes that the processing may record sensitive data within the

meaning of I of Article 6 of the law of 6 January 1978, as amended, insofar as this recording is necessary for the purpose assigned to it. These data may be recorded only to the extent that they appear in the information, data and communication content provided for in Articles R. 40-43-1 and R. 40-43-2 of the CPP. In this respect, it recalls that in accordance with article 88 of the law of January 6, 1978, the processing of such data is only possible in the event of absolute necessity, subject to the appropriate guarantees for the rights and freedoms of the concerned person . On the one hand, the Commission observes that sensitive data relating to different categories of data subjects (persons directly targeted by the measure, persons in contact with the data subject and third parties mentioned in particular during a communication for example) may be collected and retained when they are mentioned during intercepted electronic communications, during a sound system, or when they appear in the information communicated as part of a real-time geolocation measurement. The Commission notes that sensitive data can only be recorded within the framework of the implementation of a measure taken on the basis of the CPP or the customs code. It notes that these data will be kept in the PNIJ even if they prove not to be useful for the manifestation of the truth. It observes, moreover, that the deletion of all the data collected will only take place at the expiry of the limitation period for public action and that there will be no prior sorting on their relevance. . The ministry explains that it cannot be determined upstream whether the data will be useful to the investigation before it is collected and that it is not possible in real time to hide such information if it were not. not the case or even more, a posteriori, to modify the recording or the data, pledge of their integrity and, by extension, of their loyalty as proof. The Commission also takes note of the Ministry's clarifications according to which guarantees are provided, in particular the fact that interceptions and real-time geolocation are carried out under the authority and control of the magistrate for offenses presenting a certain level of seriousness and for a limited period, that only the elements useful for the manifestation of the truth are transcribed in accordance with article 100-5 of the CPP, that the interception and recording operations are the subject of minutes and that Interception measures are excluded for certain professions (journalists and lawyers in particular). The ministry also clarified that any attack on the integrity of the data stored in encrypted form until the end of the public action would risk harming both the exercise of the rights of the defense and the right to a trial. fair.While the Commission is aware of the difficulties mentioned above and takes note of the technical and procedural guarantees, it nevertheless recalls that it will be up to the Ministry to ensure that the data collected is not excessive within the meaning of the provisions of 3° of article 4 of the amended law of January 6, 1978. On the other hand, the Commission points out that information may be transcribed in areas of free fields, these being likely to contain sensitive data. It

therefore considers that it would be appropriate to pre-populate these free fields with information relating to the way in which they should be filled in and recalls that strict control must be ensured in this respect, in particular in order to ensure that only the elements useful for the manifestation of the truth within the framework of the measure ordered only are actually informed. It also recalls that, in accordance with article 94 of the law of January 6, 1978 as amended, personal data based on facts must be distinguished, as far as possible, from those based on personal assessments. Thirdly, the Commission notes that the voice recognition system, which has not yet been deployed, will not be systematically implemented and that the information relating to the speaker's voice recognition will only be recorded when this functionality will be used. It notes that this device will only be able to make it possible to recognize a person in comparison with subsequent voice interceptions received solely within the same case and that no other database will be used.Fourthly, the Commission takes acknowledgment that real-time geolocation devices can be installed on any type of structure, vehicle or object and thus concern any natural person being the target thereof. It further notes that requisitions concerning geolocation measures are not limited to persons suspected of having committed an offence, but may be brought against any individual in connection with the investigation and as long as the necessities I 'demand.In view of the foregoing, the Commission calls on the vigilance of the Ministry on the need to provide guarantees for the recording of sensitive data.The other categories of personal data collected do not call for any additional observation of on the part of the Commission. On the storage period for logging data The Commission notes that the draft decree does not modify the storage period for logging data, which is five years. The Commission points out, however, that a storage period five-year-old newspapers does not comply with the six months recommended by the Commission for this type of processing, and that no regulatory provision e justifies the application of a duration different from that usually recommended by the Commission. Furthermore, the Commission notes that it appears from the details provided by the Ministry that no log monitoring tool is deployed. It recalls that the implementation of a proactive mechanism for automatic control of traces contributes to the detection of abnormal behavior by the automatic generation of alerts and is therefore, therefore, necessary. The absence of a proactive control tool cannot be de facto compensated for by extending the retention periods for logs. The Commission therefore considers, in the light of the information at its disposal, that the retention period of five years is excessive and recalls that it recommends a duration of six months. If it were determined that significant residual risks remained despite the implementation of a proactive log control tool, the ministry could then consider increasing this duration in order to cover the identified risk. On the rights of data subjects The draft article R. 40-55 of the CPP specifies the procedures for

exercising the rights of data subjects and provides that the rights to information, access, rectification, erasure and limitation of the data mentioned in article R. 40-46 are exercised directly with the head of department, director of the ANTENJ, without prejudice to the provisions of the code of criminal procedure in the matter and the provisions of article 111 of the Data Protection Act . Firstly, the Commission thus notes that the rights of access, rectification, erasure and limitation of data may be subject to restrictions pursuant to 2° and 3° of II and III of article 107 of the said law. It takes note of the clarifications provided by the ministry according to which, for the persons listed in the PNIJ under contact with the target person or under a questioning following which no prosecution will only be initiated for cases in which it cannot be applied to article 111 of the amended law of January 6, 1978 or the rules of the code of criminal procedure, the right of access will be systematically refused due to practical and technical difficulties related to the partitioning of cases and the encryption of data which make it impossible to query by name. Without calling into question the practical and technical difficulties mentioned by the Ministry, the Commission recalls that the methods of exercise of rights must be assessed on a case-by-case basis and cannot be systematically refused. It therefore invites the Ministry to redefine these methods so as not to deprive the persons concerned, in principle, of their right.Secondly, the draft decree provides that the right of opposition does not apply to this processing, which does not call for comment. On the other conditions for implementing the planned processing On the retention periods of data Article R. 40-49 of the CPP as amended provides that the retention period for recorded data and information in the processing corresponds to the limitation period of the public action once the data has been placed under seal. The data mentioned in 3° of article R. 40-46 of the CPP as well as the information relating to the voice recognition of the speaker are also placed under seal within the processing until the expiry of the limitation period for public action when they appear useful for the manifestation of the truth. The other data and information are c retained until the closure of investigations into electronic communications. The Commission considers that the duration of data retention appears proportionate with regard to the purposes assigned to the processing. On users and recipients Firstly, the new wording of the article R. 40-47 of the CPP modifies the list of accessors to the PNIJ as well as the accesses of certain already existing recipients. have access to all the data stored there since they can only access the business for which they are registered as holder or co-holder. In addition, the data making up the responses to the requisitions are made available only to users holding the right of access to the case. In this respect, it calls the attention of the Ministry, in view of the great sensitivity of the data recorded in the processing, on the need to manage with the greatest vigilance the authorizations of the personnel concerned, in order to limit to what is strictly

necessary the persons who may have direct access to the data. More specifically, the Commission notes that the draft decree provides that judicial police officers, who only have a right of consultation, will now be able to use the PNIJ to send requisitions to electronic communications operators, in accordance with what is provided for by article 47 of law n ° 2019 -222 cited above. Customs officers authorized to carry out customs investigations for the purposes of the missions referred to in Article 67 bis-2 of the Code of s customs authorities have also been added to the list of accessors to processing pursuant to article 230-45 of the CPP. taking into account business needs: specialized assistants have been added to the list of users accessing the processing in order to allow them, via the platform, to implement their power of requisition to electronic communications operators. Indeed, it appears from the aforementioned law n ° 2019-222 that they can receive delegation of signature for the requisitions provided for by articles 60-1, 60-2, 77-1-1, 77-2-1, 99 -3 and 99-4 of the PPC. It acknowledges that legal assistants, within the meaning of decree no. 2017-1618 of November 28, 2017, as well as legal assistants do not belong to this category and cannot be accessing or receiving personal data recorded in the PNIJ; the access of clerks, which was already provided for by the CPP, has been extended to all the data contained in the processing which relate to the procedures of which they have to know insofar as their mission, in particular at the stage of the investigation, is not limited to seals; access is provided for the investigators of a requesting State, within the framework of the execution of a European investigation order or a request formulated under the 18 of the aforementioned convention of May 29, 2000, in order to facilitate the use of the results of these interceptions. el, an authorization from the magistrate seized of the procedure or from the director of the ANTENJ will be necessary. It also notes that, for the interpreters-translators as well as for the investigators of a requesting State, this access will be made by the provision of secure laptop computers allowing access to interceptions contained in the PNIJ previously selected by the holder or co-holder of the business concerned.Secondly, the Commission notes that, within the framework of the requests for interception of communications formulated under article 18 of the convention of May 29, 2000 mentioned above, transfers data outside the European Union could be achieved with Iceland as well as Norway. It also observes that the United Kingdom is no longer part of the European Union but benefits from the framework of the European investigation order on a provisional basis. In this respect, it recalls that transfers of data to States do not not belonging to the European Union can only be operated subject to compliance with the conditions set out in article 112 of the law of January 6, 1978 as amended. Where appropriate, appropriate safeguards for the protection of personal data should in particular be provided by a legally binding instrument. In the absence of an adequacy decision adopted by the European Commission or of

appropriate guarantees, and by way of derogation from the aforementioned article 112, such transfers can then only be carried out subject to compliance with the conditions set out in article 113. of the amended law of 6 January 1978. Subject to the foregoing, the Commission considers that the consultation of the data by the persons mentioned in the new articles appears justified and proportionate. On the right to information of the persons affected by the measures and indirectly concerned as well as the users of the PNIJ With regard to the information of the persons concerned, the Commission considers that the wording of the draft decree relating to the right to information is ambiguous and should be clarified insofar as, in accordance with article 104-I of the law of January 6, 1978 as amended, it is the responsibility of the data controller to make available to the person concerned the information ions listed and not up to the person to request communication of this information. It takes note of the ministry's commitment to modify the wording of the draft decree accordingly. The Commission notes that the right to information will be differentiated according to the categories of persons concerned, depending on whether these persons are users of the platform. -trains or the persons targeted directly or indirectly by the measures listed in draft article R. 40-46 of the CPP. With regard to users of the PNIJ, it observes that three modalities are thus provided for the right to information: details provided in the user guide, changes to the PNIJ homepage so that the information is easily available and information on the intranet page of the Ministry of Justice. For the persons concerned by the measures and indirectly concerned, it notes that the right to information may be subject to restrictions pursuant to article 107-II-1° of the law of January 6, 1978 as amended in order to avoid interference negate inquiries, investigations or legal proceedings, to prejudice the prevention, investigation or prosecution of criminal offenses or the execution of criminal penalties and to protect public safety. It acknowledges that the information will be published on the website of the Ministry of Justice. On security measures Access to PNIJ processing is via a WEB interface and in different ways depending on the user: for users belonging to one of the ministries having access to the processing, the use of the agent card is compulsory in order to authenticate on the application and to have access to it; for the administrators of the PNIJ, access to the processing is using dedicated workstations based on the CLIP secure operating system, provided by ANSSI, qualified as restricted distribution and implementing cryptographic mechanisms to secure data; for interpreters-translators, in charge of translation elements collected, access is achieved using CLIP workstations substantially identical to those used by the subcontractor chosen by the Ministry of Justice. On the conditions of access to processing, the Co mmission notes that, overall, the level of security provided is adequate and that potential weaknesses have been identified and are being dealt with. population of users concerned. The Commission recalls, in the event that agents or administrators

have to authenticate themselves using an identifier and password pair, which it elaborated in its deliberation n° 2017-012 of January 19, 2017 adopting a recommendation relating to passwords as well as in its deliberation no. 2017-190 of June 22, 2017 amending the recommendation relating to passwords, several recommendations relating to the use of this technique authentication. It therefore invites the Ministry to read it and to make any necessary changes in order to bring its password policy into line with the Commission's recommendations. The Commission therefore recommends that the systems incorporate a renewal request function passwords regardless of the population concerned. Similarly, the Commission recommends eliminating, as far as technically possible, the use of generic accounts. In addition, the Commission encourages automatic disconnection of accounts, both users and super-users, after a period of inactivity, the duration of which must not be excessive depending on the context. Finally, with regard to logical accesses, the Commission recommends, in order to limit the attack surface, to delete any existing application part that is not useful within the final application, in particular with regard to the parts relating to portals s of access. The Commission takes note of the encryption measures implemented at the level of the flows, as well as the management of the latter, and has no particular comments to make on this subject. The Commission recommends, on the management traces and technical logs, to implement a retention period not exceeding six months, except to be able to prove that certain risks can only be covered by an extension of this period, and to implement, with a view to to be able to ensure the integrity and availability of the latter, a system for centralizing traces. The Commission points out that proactive monitoring of technical logs is necessary and that the absence of tools cannot justify a extension of the retention period for these logs. President Marie-Laure DENIS