Deliberation 2018-310 of September 13, 2018Commission Nationale de l'Informatique et des LibertésType of deliberation: OpinionLegal status: In force Date of publication on Légifrance: Saturday November 24, 2018NOR: CNIX1832020XDeliberation No. 2018-310 of September 13, 2018 providing an opinion draft decree creating an automated processing of personal data called "platform for reporting sexual and gender-based violence" (request for opinion no. 18014530)The National Commission for Computing and Liberties,

Seizure by the Minister of the Interior of a request for an opinion on a draft decree creating an automated processing of personal data called a platform for reporting sexual and gender-based violence;

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 penal code;

Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its article 26-II and its chapter XIII;

Having regard to Law No. 2018-703 of August 3, 2018 strengthening the fight against sexual and gender-based violence;

Considering the decree n° 2005-1309 of October 20, 2005 modified taken for the application of the law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms;

Having heard Mr. Jean-François CARREZ, commissioner, in his report, and Mrs. Nacima BELKACEM, government commissioner, in her observations, Issues the following opinion:

The commission has been asked by the Minister of the Interior for an opinion on a draft decree creating an automated processing of personal data called a platform for reporting sexual and gender-based violence. In a context of strengthening fight against sexual and gender-based violence resulting in particular from the adoption of law n° 2018-703 of August 3, 2018, this platform must allow victims or witnesses of this violence to be directed to specially trained police officers or gendarmes , and to exchange with them in real time using an instant conversation tool (real chat). The committee thus notes that the

purpose of the planned treatment is to improve the care and referral of victims to the competent services in order to facilitate any subsequent filing of a complaint with these same services. In this respect, it stresses that when the facts are likely to be criminally qualified and to lead to the opening of legal proceedings, the data recorded under the report is transmitted to the software for drafting the procedures of the national gendarmerie or of the national police, on which the commission has already ruled. the national police and gendarmerie. In this respect, it stresses that the mechanism as it is to be implemented is only a temporary solution, the timetable and nature of the changes to which have not been precisely communicated to the committee. However, the Ministry has indicated that the purposes and the main characteristics of the processing are not intended to change.

It recalls, however, that it must be kept informed and seized, under the conditions provided for in Article 30-II of the law of January 6, 1978, of any development relating to new functionalities of the device and in particular, the development of new tools. allowing the cross-checking of reports. In the same way, it underlines that the impact analysis transmitted to the commission, under the conditions provided for in article 70-4 of the aforementioned law, will have to be updated.

Finally, it takes note of the commitment made by the ministry to provide it, after the first year of the system's launch, with an assessment of the operation and operational use of the platform. In this respect, it asks that it be provided with, in addition to general elements on the implementation of the service, any information relating to the operational needs identified during the implementation of the platform and future developments of the tool. Insofar as the purpose of the processing is the prevention, research, observation or prosecution of criminal offences, and where the data mentioned in I of article 8 of the law of January 6, 1978 as amended are likely to be recorded in the processing, this must therefore be the subject of a decree in Council of State, taken after reasoned and published opinion of the commission in accordance with the provisions of article 70-3 of the law of January 6 1978 modified.

On the purposes of the processing

Article I of the draft decree sets out the purposes pursued by the processing, namely:

- allow a minor or adult, believing to be a victim or witness of sexual or gender-based violence, to enter into a relationship and exchange by instant messaging with national police personnel or a soldier of the national gendarmerie and to make a report, from a teleservice made available to them on the service-public.fr site;

- collect the reports mentioned and send them to the territorially competent investigation services;

- inform, guide and facilitate the handling of the person who considers himself to be a victim or witness of the facts falling within the scope of the platform by the competent authorities, taking into account any previous reports.

The commission notes first of all that the implementation of this platform aims to improve the care of victims by offering a solution available seven days a week and twenty-four hours a day, the scope of which aims to include numerous sexual or sexist offenses as defined by the provisions of the penal code (such as sexual assault, sexist insult or corruption of a minor). In this respect, it specifies that the planned processing differs from an online pre-complaint system, the reporting person not being required to follow up on his report and the information transmitted by it being simply declarative in nature. The committee also notes that minors are likely to use the reporting platform. It acknowledges that, in this case, increased attention will be paid to listening to and taking their situation into account, in accordance with the training given to operators.

The commission considers that the purposes pursued by the planned processing are determined, explicit and legitimate, in accordance with article 6 (2°) of the law of January 6, 1978 as amended.On the data collected

As a preliminary point, the commission notes that, prior to any report, the declarant must enter his postal code as well as his municipality of residence. It acknowledges that these data are only intended to direct it to the territorially competent services and that as such, they will not be the subject of any recording in the planned processing.

The commission also notes that only the data of the conversations in connection with the purposes of the platform will be the subject of a recording in the processing, and this, for the purpose of manual transmission to the software for drafting the procedures of the gendarmerie. national or national police using the secure intranet messaging system of the Ministry of the Interior. The commission takes note that the permanent solution which must be implemented in a second time by the ministry must make it possible to automatically feed the various business tools of the services identified as competent. It recalls in this respect that, in the event of an evolution of the device, in particular for the purpose of interconnecting the platform with the software for drafting procedures, all of the processing referred to will have to be modified, submitted for opinion to the commission, under the conditions provided for in article 30-II of the amended law of January 6, 1978.

Article 2 of the draft decree lists the categories of personal data and information recorded in the processing, distinguishing between those relating to the declarant, the agent in charge of processing the report sent and the facts reported. Firstly, concerning the reporting person, the following may thus be collected: the surname, first name, address, telephone number, e-mail address, IP address and source port of the person concerned. The commission notes that the collection of data relating

to the declarant's IP address and source port is intended to allow the police to intervene, in the event of a proven emergency situation , and in which the signaling party would not have communicated his location or if he would, for example, be unable to call the emergency services directly.

Given the justifications provided by the ministry on the reasons leading to the collection of such data, which, when the system was presented, were subordinated to the sole hypothesis of an immediate intervention by the police, the commission considers that the data relating to the declarant's IP address and source port should be deleted when the report is closed, in all cases where the police have not intervened, in order to limit the risk of re- identification of the persons concerned. The ministry now intends to take advantage of new cases of use making it possible to justify the conservation of this data, namely, the need to identify the reporting person: in the event of a technical interruption of the conversation, in the context of malicious use of the service for the purposes of possible prosecution for contempt or even the hypothesis of a false or slanderous denunciation in order to allow the person in question to t file a complaint. The commission takes note of the new reasons invoked by the ministry, such as to justify the collection and storage of this data for a limited period. It notes, however, that the assumptions in which this data will be used are such as to greatly reduce the possibility for reporting persons to use the platform anonymously.

Secondly, the draft decree provides that data relating to the platform agent handling the report, are recorded. These data, relating to the surname and first name, the quality, the service or the unit of assignment of the agent, as well as the professional e-mail address of the latter, do not call for comments. of the commission.Thirdly, the draft decree specifies that, with regard to the data relating to the reported facts, can be collected: the nature and the circumstances of the facts, the data relating to the persons concerned (surname, first name, address, telephone number, e-mail address, as well as other identification or contact details), the quality of these persons (perpetrator, witness, victim), the date, time and place of commission of the facts. The collection of this data does not call for any particular observations on the part of the committee.

Fourthly, article 3 of the draft decree provides that the processing may record data of the nature of those mentioned in I of article 8 of the law of January 6, 1978 referred to above and relating to the alleged racial origin or ethnic origin, political opinions, religious beliefs, trade union membership, health or concerning the sex life or sexual orientation of a natural person, insofar as these data are necessary for the prosecution purposes mentioned in Article 1. Paragraph 2 of this article provides that it is prohibited to select in the processing a particular category of persons from these data alone. The commission recalls that in accordance with article 70-2 of the law of January 6, 1978 , the processing of such data is only possible in cases of

absolute necessity, subject to appropriate safeguards for the rights and freedoms of the data subject. In this regard, it notes that the Ministry has indicated that these data must enable the persons concerned to use the instant chat tool and that it cannot be ruled out that their collection proves necessary to qualify the aggravating circumstances of certain offenses falling within the scope of the platform. In any case, it takes note of the guarantees surrounding the processing of this sensitive data, namely that it will not be possible to carry out a search full text within the platform from these data, which cannot be extracted, in particular for the purpose of compiling statistics. The commission notes that these guarantees will remain unchanged under the permanent solution.

It also stresses that the agents in charge of managing reports within the platform must be specifically made aware of the collection and processing of this type of data, during the training that will be provided to them. that the reports made by the declarant do not require him to identify himself by means of his surnames and first names. In general, and without calling into question this possibility of recourse to anonymity, it recalls that it is appropriate, taking into account the purposes pursued by the processing, not to encourage them and to treat them with precaution. The commission notes that , in the context of a report made anonymously, the system as currently envisaged allows operators to access the history of reports of the person concerned when the latter communicates the date of their previous exchanges. The operator then accesses it via the procedures drafting software tools by carrying out a manual, non-automated search from the date of the report transmitted.

The commission points out that it should be informed of any changes in the technical methods allowing access to the history of conversations. Finally, it notes that, contrary to what was initially envisaged, it will not be possible to make a report after having identified oneself via social networks. Under these conditions, the commission considers that the categories of data referred to in articles 2 and 3 of the draft decree and recorded in the processing are adequate, relevant and not excessive, in accordance with the provisions of article 6 (3°) of the modified law of January 6, 1978. On retention periods

The commission recalls first of all that the system, in its first version, provides that the data is kept in the instant conversation tool for the time strictly necessary for the report, i.e. a period which cannot exceed four hours after the close of a conversation, and at the end of which the data is deleted after transmission to the procedures drafting software.

Article 4 of the draft decree provides that in a later stage, the personal data and information mentioned in article 2 are kept for a period of six years from their registration. The ministry indicated in this respect that Such a duration appears justified, insofar as it corresponds to the limitation period for public action in tort. He also specified that the purpose of keeping this data within

the platform is to allow operators to access the history of a person's reports, in the event that the latter has not communicated sufficiently elements allowing the initiation of legal proceedings and on which it would like to provide additional information. The Committee notes that, when the reports have been the subject of the opening of legal proceedings, data for the sole purpose of making it possible to complete a first report is devoid of any justification, the legal procedure being precisely intended to collect all the necessary information. Therefore, this data should be deleted as soon as it is transmitted to software for writing police and gendarmerie procedures, during the development of the permanent system. the initiation of a procedure, the retention of data relating to the facts reported may be justified to allow the reporting party to complete his first description. Finally, the commission recalls that the IP address as well as the source port will also be kept for a period of six years. Given the purposes invoked by the Ministry to justify the collection and storage of this data, it considers that such a duration is disproportionate.

In view of all of these elements, and without calling into question the operational needs expressed by the services, the commission considers that the retention of data, for a period of six years, is manifestly excessive. further that, if general information on the existence and characteristics of the treatment will be publicly available on the Ministry's website and in the general conditions of use of the platform, the persons who, as author or witness, made the object of these reports will not be informed. If this absence of information is justified by the purpose of the processing, which is the investigation and prosecution of criminal offences, the storage for a long period, without the knowledge of the persons concerned, of reports relating to very sensitive incriminations is likely , in the event of accidental or deliberate dissemination, to cause serious harm to the persons concerned, which reinforces the need for a limitation of the retention period. On the recipients

Article 5 of the draft decree provides that only have access, by reason of their attributions and within the limits of the need to know, to all or part of the personal data and information recorded in the processing, personnel of the national police and the soldiers of the national gendarmerie responsible for collecting reports, individually designated and authorized by the heads of the territorial services of the national police or by the commanders of units of the national gendarmerie. The commission takes note of this that the staff covered by the draft decree are trained beforehand in order to be able to effectively guide the person concerned and only keep the data necessary and related to the scope of the platform.

The Ministry has also proposed amending the draft decree to specify that authorized persons will only be able to access processing under strictly defined conditions, once the report has been transmitted to the competent services (processing of

reports, operations carried out within the framework of procedures judicial or inspection missions coming under this ministry). It is noted. In view of these elements, it considers that the access of these persons to the data recorded in the processing is justified.

In addition, article 5 of the draft decree provides that other categories of persons may be recipients of the data recorded in the processing. Firstly, it is provided that police personnel and national gendarmerie soldiers responsible for of the processing of the report may be recipients of the data of the processing, by reason of their attributions and within the limit of the need to know. These categories of people do not call for any particular observations on the part of the commission. Secondly, this same article specifies that magistrates may be recipients of this same data. In this respect, the commission considers that the mere mention of the expression magistrates does not make it possible to determine with sufficient precision the persons concerned as well as the circumstances in which the data are actually transmitted to them. In this regard, it takes note that the draft decree will be amended so that the magistrates of the public prosecutor's office or those responsible for the investigation are referred to for the facts of which they are seized. Under these conditions, it considers that it is justified that these people are recipients of the data recorded in the processing. Thirdly, the partners associated by the personnel of the national police and the national gendarmerie responsible for collecting reports and coming victim support system may be recipients of the data recorded in the processing under the conditions of article 5 of the draft decree. This category is aimed more particularly at psychologists and social workers in police stations or gendarmerie units, whose missions relate in particular to improving the quality of the reception of victims and relations with the population. As such, they are intended to be recipients in particular of data relating to the identity of the person concerned and the facts reported in order to allow contact and possible support for the person who wishes it.

With regard to the missions entrusted to them, the commission considers that it is justified that these personnel are recipients of the data recorded in the processing. It also takes note of the commitment of the ministry to specify the wording of article 5- II (3°) of the draft decree making it possible to define these personnel more precisely and thus target the personnel covered by the victim support system assisting the police responsible for collecting reports employed by an association or organization having signed a provision and partnership agreement with the State in the context of the exercise of victim assistance missions. On the rights of the persons concerned

The commission notes that general information will be issued to the public via the general conditions of use, accessible on the

platform. In addition, information on the treatment will be issued on the ministry's website. The commission notes that the link to the general conditions of use, which is automatically displayed in the first input field of the instant messaging service, remains visible on the screen for the duration of the conversation between the declarant and the operator. However, and given the very purpose of the processing, the persons mentioned by the reporting as author or witness will not have information on the fact that they are the subject of a report, nor on the declarant who calls them into question, neither on the facts likely to be imputed to them, nor on the conservation of these elements for a period currently set at six (6) years.

The persons concerned can exercise their rights of access, rectification and erasure directly with the general management of the national police and the general management of the national gendarmerie. It is however provided that restrictions are possible and this, under the conditions of I and 2° and 3° of II of article 70-21 of the law of January 6, 1978 modified. In this hypothesis, these rights work indirectly with the National Commission for Computing and Liberties under the conditions provided for in Article 70-22 of the aforementioned law.

The commission notes that the exercise of the rights of access, rectification and erasure of the persons mentioned as author or witness by the informant in the processing, will in practice be greatly limited insofar as they will not have, in principle, not intended to have knowledge of the report against them. Finally, the draft decree specifies that pursuant to article 38 of the law of January 6, 1978 as amended, the right of opposition is not intended to apply to the planned processing. implementation, the Member States retain, in any event, the possibility of providing more extensive safeguards than those established in the said directive for the protection of the rights and freedoms of data subjects with regard to the processing of s personal data by the competent authorities. In this context, it considers that the aforementioned Article 38, which has not been repealed by the law relating to the protection of personal data and whose application to processing under the aforementioned directive is not excluded by the provisions of articles 70-1 and following of the Data Protection Act, is also intended to apply to processing falling within the scope of this directive. It notes in this respect that Article 38 provides for the possibility of disregarding the right of opposition when the processing meets a legal obligation or when an express provision of the regulatory act authorizing the processing excludes it. , the commission considers that the exclusion of the right to object as provided for in article 7 of the draft decree is proportionate with regard to the purpose pursued by the planned processing, namely the collection of reports of violence of a sexual nature and sexist and their transmission to the territorially competent investigation services. In view of the foregoing, it considers that the limitation imposed on the exercise of the right to object falls within the framework of the

provisions of national law relating to the protection of personal data and is not likely to excessively interfere with the rights and freedoms of data subjects. On security measures

The commission notes first of all that access to the teleservice will be via the HTTPS protocol, and recalls its recommendation to use for this the most up-to-date version(s) of TLS possible. In this context, the commission recalls that it is up to the ministry to formally certify the acceptance of the security level of the teleservice through a general security reference standard (RGS) approval as provided for by decree no. 2010-112 of February 2, 2010 and to publish the certificate of approval on its site. Authorization profiles are also provided in order to manage access to data as needed. The commission takes note of the ministry's commitment to ensure compliance, in particular by its service provider, with deliberation no. 2017-012 of 19 January 2017 adopting a recommendation relating to passwords amended by deliberation no. 2017-190 of June 22, 2017, and this in particular with regard to the storage of passwords. A logging of the operations of creation, modification, consultation, communication, transfers and deletion of data is put in place. The committee recalls that unless specifically justified, the shelf life it recommends is six (6) months. While it takes note of the elements provided by the Ministry, it considers that a period of less than six (6) years could have been adopted with regard to the conservation of these logs. In any case, and in order to limit the risks of non-detection of abnormal use of the device, the commission recommends carrying out an automatic control of the traces, generating alerts if necessary, as well as a regular review. authorizations and checks on their use. The commission considers that the temporary solution involves storing the data with a service provider that does not ensure the level of guarantee usually desired for this type of processing. It notes that in order to limit the risks generated by this architecture, the data will be encrypted on the server and deleted within four hours. The committee also takes note of the ministry's commitment to choose, for the long-term solution, a system that guarantees a high level of security as required by the nature of the processing. Finally, the committee notes that the ministry has implemented several measures to limit the risk for the victim of a discovery of their use of the platform by a third party.

Subject to the previous observations, the security measures described by the data controller for the temporary solution comply with the security requirement provided for by article 70-13 of the law of January 6, 1978 as amended. The commission recalls, however, that this obligation requires the updating of security measures with regard to the regular reassessment of risks. In this respect, it recalls in particular that specific attention should be paid to the reassessment of security measures within the framework of the imperative update of the impact analysis.

The president,

I. Falque-Pierrotin