Deliberation 2020-052 of May 14, 2020Commission Nationale de l'Informatique et des LibertésNature of the deliberation: OpinionLegal status: In force Date of publication on Légifrance: Wednesday July 01, 2020NOR: CNIX2016618XDeliberation n° 2020-052 of May 14, 2020 providing an opinion on a draft decree creating an automated processing of personal data called "harmonized processing of investigations and reports for e-frauds" (THESEE)The National Commission for Computing and Liberties,

Seizure by the Minister of the Interior of a request for an opinion concerning a draft order creating an automated processing of personal data called harmonized processing of investigations and reports for e-frauds (THESEE);

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 Code of Criminal Procedure, in particular its article 15-3-1;

Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its article 89;

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 Decree No. 2011-110 of January 27, 2011 authorizing the creation of an automated processing of personal data called National Police Procedures Drafting Software (LRPPN);

Having regard to decree n° 2011-111 of January 27, 2011 authorizing the implementation by the Ministry of the Interior (General Directorate of the National Gendarmerie) of an automated processing of personal data to assist in the drafting of procedures (LRPGN);

Considering the decree of February 24, 2016 relating to the integration into the service public.fr website of a teleservice allowing the user to carry out administrative procedures in whole or in part dematerialized and to have access to personalized information services;

Having regard to the decree of November 8, 2018 relating to the teleservice called FranceConnect created by the interministerial department of digital and the State information and communication system;

Having heard Mrs. Sophie LAMBREMON, commissioner, in her report, and Mrs. Nacima BELKACEM, government commissioner, in her observations, Issues the following opinion:

The draft decree submitted for opinion to the Commission aims to provide a framework for the creation of a harmonized processing of investigations and reports for e-frauds (THESEE). This processing is intended to constitute the first online complaint mechanism set up pursuant to Article 15-3-1 of the Code of Criminal Procedure (CPP), introduced by Law No. 2019-222 of March 23, 2019 of 2018-2022 programming and reform for justice.

According to the Ministry, the implementation of this processing, which is part of a context of a sharp increase in offenses committed on the Internet, aims to facilitate the procedures for victims and the work of investigators by modernizing the complaint and reporting procedures in this domain. The Commission takes note of the clarifications provided by the Ministry according to which the THESEE system will be governed by three separate regulatory acts:

- the decree authorizing the creation of the processing of personal data that is the subject of this referral;
- a joint order of the Ministers of the Interior and of Justice setting the list of offenses for which it will be possible to file a complaint online, taken for the application of Article D. 8-2-1 of the CPP;
- an order of the Minister of the Interior relating to the methods of secure identification adopted. Insofar as the THESEE processing is implemented for the purposes of prevention and detection of criminal offences, investigations and prosecutions in this area , the Commission considers that the processing falls within the scope of the aforementioned Directive (EU) 2016/680 of April 27, 2016 and must be examined in the light of the provisions of Articles 87 et seq. of the law of January 6, 1978 as amended. It observes, however, that this processing should allow the production of statistics relating to online e-scams, in order to guide the strategy for combating these offences. In this context, the Commission recalls from the outset that it will be up to the Ministerial Statistical Service for Internal Security (SSMSI), in its capacity as data controller in this context, to ensure compliance with the applicable regulations of its data processing operations.

Insofar as the planned processing is likely to create a high risk for the rights and freedoms of natural persons, the Ministry of the Interior has carried out an impact assessment relating to the protection of personal data (AIPD), which was sent to the Commission with the request for an opinion in accordance with article 90 of the amended law of January 6, 1978. On the

general conditions for implementing the system and the purposes of the processing:

The Commission notes first of all that the purpose of THESEE processing is to allow a victim to make a complaint or report only from a teleservice made available to him on the service-public.fr website for acts committed on the Internet. and falling within the criminal scope of fraud, blackmail or extortion. In practice, it takes note of the clarifications provided by the Ministry according to which the operating methods specifically and exclusively targeted by this processing are as follows:

- romance scam on the internet;

- Internet classified ad scam;

- scams on fake online sales sites;

- fraud related to an attack on automated data processing systems (use of stolen data, use of a pirated mailbox, etc.);

- blackmail on the internet;

- extortion related to an attack on automated data processing systems (hacking of a computer or any other information system accompanied by a ransom demand through ransomware). Article 1 of the draft decree specifies as such, only complaints and reports filed by adult and capable victims and directed against an unknown perpetrator are concerned by the system.

It acknowledges that access to the complaint forms, after an initial orientation questionnaire to ensure that the conditions for using the THESEE system are met, will be conditioned by the identification and authentication of the user. via the FranceConnect system, on which the Commission has ruled on several occasions.

With regard to the possibility of making a report, the Commission notes that the user will benefit from three possibilities: to make a report anonymously, to declare his identity or to authenticate himself via the FranceConnect solution.

Finally, it recalls that the victim will always have the possibility of going to the police station or the gendarmerie brigade to file a complaint. In this case, the report is signed electronically and data from this report may subsequently be transmitted to the THESEE unit in order to allow the analysis and cross-checking of this data with that recorded in the processing.

The Commission notes that the phase of validation of complaints and reports by agents of the Central Office for the Fight against Crime linked to Information and Communication Technologies (OCLCTIC) should make it possible to exclude from the tool of analyzes data from incorrectly completed forms, complaints or reports that do not contain the constituent elements of a criminal offense eligible for the THESEE system or a declaration already made by the user.

It also notes that the planned processing must allow:

- to centralize on a national platform all the complaints concerning the aforementioned offences, whether they have been filed online by means of the teleservice, or with the territorial police or gendarmerie services, as well as the reports made through the teleservice before leading to their exploitation and a cross-checking of the data thus collected by the specialized investigators of the OCLCTIC;

- the competent judicial authorities to inform the victims of the follow-up reserved for their complaint within the framework of the electronic communication in criminal matters provided for in article 803-1 of the CPP, thus contributing to simplifying relations between users and the judicial authorities ;

- to have statistical data relating to e-scams to guide the strategy for combating these offences. In view of these elements, the Commission considers that the purposes pursued by the processing are determined, explicit and legitimate, in accordance with the article 4-2° of the amended law of January 6, 1978. On the data collected: Firstly, with regard to the facts likely to guide the investigation, the Commission notes that only the data transmitted by the victims in the their complaint or their report will be recorded in the THESEE processing and that, consequently, no data resulting from the investigations of the investigators will feed the latter.

The Commission notes that Article 2 of the draft decree provides, among the data collected relating to the person in question, or relating to a person in contact with the latter, the recording of data such as surnames, first names, pseudonyms, e-mail addresses, postal address, telephone numbers, names of profiles on social networks. Insofar as the primary purpose of THESEE processing is to allow cross-checking of complaints and reports against unknown perpetrators, in order to facilitate the identification of the latter, it recalls the importance of ensuring that the investigators required to intervene at the stage of validating the information transmitted by the victims will in no way register, in THESEE, data relating to a precisely identified offender.Secondly, the Commission notes that the collection of categories of information and data mentioned by the draft decree will be carried out by means of questionnaires comprising free fields. It notes in this respect that no filter device is provided to prevent the transmission or to delete any irrelevant or sensitive data that a presumed victim would have mentioned in these fields or would have communicated through other elements collected via teleservice, such as images of discussions or electronic exchanges.

The Commission observes first of all that the data thus collected is likely to concern both the persons implicated and the victims making a complaint or report and takes note of the ministry's commitment to include a specific mention in the proposed

questionnaire in order to invite the person not to enter sensitive data in the free field.

While it also takes note of the justifications provided according to which the absence of a filter must make it possible not to distort, modify or delete the statements that a potential victim would like to bring to the attention of the courts, the Commission underlines that with regard to the planned device, it is not possible to exclude that sensitive data within the meaning of article 6 of the law of January 6, 1978 as amended will be collected. It recalls that in such a case, it would be appropriate to apply the provisions of Articles 31 and 88 of this same law, which make the implementation of processing relating to this specific data subject to authorization by decree in Council of State taken after opinion of the Commission, and only where absolutely necessary and subject to appropriate safeguards for the rights and freedoms of the data subject.

In view of the foregoing and in the absence of a change in the nature of the regulatory act, the Commission recalls that the Ministry will have to set up filtering procedures to effectively prevent the recording of such data.

Subject to these reservations, the Commission considers that the categories of data are adequate, relevant and not excessive in relation to the purposes for which they are collected. On the data retention periods:

Article 3 of the draft decree specifies that the data and information recorded in the processing are kept for six years from their recording.

The Commission takes note of the justifications provided by the Ministry according to which this duration must make it possible to cover the investigations carried out throughout the period of limitation of public action in correctional matters, which is also six years under Article L. 8 of the CPC.

It notes that if the complaints or reports made, either via the teleservice or, in the case of complaints, to the police or gendarmerie services, do not fall within the scope of the system, the data will not be not recorded in the THESEE processing analysis tool and the reporting or complainant will be notified of the reason for this rejection.

The Commission notes that the data and information relating to the complaint or the rejected report will nevertheless be kept in the procedures drafting software (LRP) and takes note, in this respect, of the clarifications provided by the Ministry according to which the conservation of such data and information must make it possible to be able to justify the rejection made if necessary. Insofar as the retention of this data has the sole purpose of justifying the rejection of a complaint or report, it recalls that the retention period of this data must be set in a manner proportionate to this purpose.

With regard to the retention period of data in the LRPs, the Ministry indicated that this is set by the regulatory act authorizing

the creation of each processing operation concerned. With regard to the LRPPN, Article 3 of Decree No. 2011-110 of January 27, 2011 referred to above sets the retention period for data at five years, from the date of transmission of the procedure to the judicial authority or competent administration. With regard to the software for drafting the procedures of the national gendarmerie (LRPGN), article 3 of decree n° 2011-111 of January 27, 2011 mentioned above specifies that the data is kept until the closure of the procedure and its transmission. to the competent judicial or administrative authority. The Commission recalls the importance of ensuring that the data collected in this way will not be kept beyond the period provided for by the provisions governing the LRPs.

Article 5 of the draft decree also provides that the traces relating to the creation, consultation, updating and deletion of data are associated with the identifier of the author of the action as well as the date, time and subject of the the object of the operation. This data is also kept for a period of six years.

If, in view of the foregoing, the retention period of the data in the THESEE processing does not call for any particular observations, the Commission recalls that with regard to the retention period of the logging data, the collection of these data has the sole purpose of detecting and/or preventing illegitimate operations on the data. The duration of storage of these traces must thus be fixed in a manner proportionate to this sole purpose, these traceability data must also in no case allow information to be obtained on data whose retention period has expired. On the others conditions for implementing the processing: On the interconnections implemented

The Commission recalls that the validation of a complaint constitutes the starting point of the procedure, which results in the drafting of a report of receipt of the complaint on the LRPs of the national police and gendarmerie authorized by the decrees of January 27, 2011 referred to above. The drafting of the complaint receipt report requires interconnection with the aforementioned software.

It notes that the interconnection of the THESEE processing with the LRP processing will allow the transmission to the THESEE unit of the complaint reports drawn up by the territorial services, when the complainants have traveled to file a complaint. In this context, the Commission recalls that the data controllers interconnected with THESEE will have to develop the processing and their documentation accordingly.

On data transfers to States not belonging to the European Union or to recipients established in States not belonging to the European Union

It follows from the DPIA transmitted that transfers of data to States not belonging to the European Union or to recipients established in States not belonging to the European Union may be carried out, in a non-automated manner, within the framework of international cooperation in matters of judicial police, pursuant to article L. 235-1 of the internal security code.

The Commission recalls in this respect that the transfer of data to these States can only be carried out subject to compliance with the provisions set out in Articles 112 to 114 of the law of 6 January 1978 as amended. About buyers and recipients

Article 4 of the draft decree details the list of accessors and recipients of THESEE processing.

The Commission notes that the following will be able to access the data:

- OCLCTIC agents;

- the magistrates of the public prosecutor's office of the place of automated processing of personal information for research relating to the offenses concerned and the agents of the judicial services acting under their authority. It notes that the following persons are among the recipients:

- the agents of the national police services and the soldiers of the national gendarmerie carrying out judicial police missions;

- the magistrates of the public ministry other than those having access to the treatment, the magistrates in charge of the instruction and the agents of the judicial services acting under their authority for research relating to the offenses and procedures of which they are seized;

- organizations for international cooperation in matters of judicial police and foreign police services;

- the Ministerial Statistical Service for Internal Security. These categories of persons authorized to access the data and these recipients do not call for any particular observations from the Commission with regard to the purpose pursued by the planned processing. On the rights of persons

The Commission notes that the information appearing in I as well as in 1°, 2° and 3° of II of article 104 of the law of January 6, 1978 as amended will be made available to the person concerned via a posting on the portal. of declaration of the service-public.fr website, as well as by an e-mail sent following the complaint or report.

Article 6 of the draft decree also provides that the right of access provided for in article 105 of the amended law of 6 January 1978 is exercised with the central directorate of the judicial police (DCPJ).

With regard to the rights of rectification, erasure and limitation of data provided for in article 106 of the law of January 6, 1978 as amended, the processing manager reserves the right not to inform the applicant of his refusal. to rectify, erase or limit data

concerning him in order to avoid hampering investigations, research or administrative or legal proceedings, or to avoid harming the prevention or detection of criminal offences, investigations or prosecutions in this area, or the execution of criminal penalties, grounds provided for in 1° and 2° of article 107 of the law of January 6, 1978.

Article 6 of the draft decree finally provides that the right of opposition does not apply to the processing, under the conditions provided for in article 110 of the law of January 6, 1978 as amended. On data security:

The Commission observes that exchanges between the user and the service-public.fr website will benefit from the security provided by the aforementioned website, in particular with regard to encryption between the user's workstation and the site, as well as authentication of the data controller. Exchanges between the site, implemented by the legal and administrative information department (DILA) and the OCLCTIC servers, will take place through the interministerial State network (RIE) and will benefit from the security provided by him.

It recalls that the teleservice envisaged is subject to the requirements provided for by Ordinance No. 2005-1516 of December 8, 2005, which creates the general security reference system (RGS), as well as by Decree No. 2010-112 of February 2, 2010 .

The other security measures do not call for any particular comments. The President,

Marie-Laure Denis