Deliberation 2019-119 of September 26, 2019Commission Nationale de l'Informatique et des LibertésNature of the deliberation: OpinionLegal status: In force Date of publication on Légifrance: Saturday January 04, 2020NOR: CNIX2000110XDeliberation n° 2019-119 of September 26, 2019 providing an opinion on a draft decree amending decree no. 2015-1700 of December 18, 2015 relating to the implementation of the processing of computer data collected pursuant to article 706-102-1 of the code of criminal procedure (request for opinion no. 18004354) The National Commission for Computing and Liberties,

Seizure by the Minister of the Interior of a request for an opinion concerning a draft decree amending decree no. 2015-1700 of December 18, 2015 relating to the implementation of the processing of data collected pursuant to article 706 -102-1 of the Code of Criminal Procedure;

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 (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention and detection of criminal offences, investigation and prosecution thereof 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 articles 28-2 and 706-95 to 706-102-9;

Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its articles 31-II and 31-IV;

Having regard to Law No. 2011-267 of March 14, 2011 on orientation and programming for the performance of internal security;

Having regard to Law No. 2014-1353 of November 13, 2014 reinforcing the provisions relating to the fight against terrorism, in particular its article 21;

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;

Having regard to Decree No. 2015-1700 of December 18, 2015 relating to the implementation of the processing of computer

data captured pursuant to Article 706-102-1 of the Code of Criminal Procedure;

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;

Considering the decree of May 9, 2018 creating the service with national competence called the national technical service for judicial capture;

Having regard to deliberation no. 2015-109 of April 2, 2015 providing an opinion on a draft decree relating to the implementation of captured data processing systems On the proposal of Mrs. Sophie LAMBREMON, commissioner, and after having heard the observations of Mrs. Nacima BELKACEM, Government Commissioner,

Gives the following opinion:

The Commission received a request for an opinion from the Minister of the Interior on a draft decree amending decree no. 2015-1700 of 18 December 2015 relating to the implementation of computer data processing captured pursuant to Article 706-102-1 of the Code of Criminal Procedure (CPP).

This processing, on which the Commission has already ruled in its aforementioned opinion no. 73-1 of the [CPP], the collection of evidence of these offenses and the identification of their perpetrators by means of the collection, recording and storage of captured computer data.

Insofar as the processing operations concerned are implemented for the purposes of prevention, detection of criminal offences, investigation and prosecution in this area, and that sensitive data, within the meaning of Article 6 of the amended law of January 6, 1978 are likely to be collected and recorded, their modification must be the subject of a decree in Council of State, taken after reasoned and published opinion of the Commission. The draft decree examined also constitutes a single regulatory act, in reference to which compliance commitments will be sent to the Commission prior to each implementation of the processing of captured computer data, in accordance with the provisions of Article 31-IV of the amended law of January 6, 1978. In this respect, the Commission takes note of the clarifications provided by the Ministry according to which only the general directorates of the national police (DGPN), the national gendarmerie (DGGN), internal security (DGSI), as well as customs and duties (DGDDI) are likely to implement such processing.

It also considers that it follows from the development of the legal framework relating to the protection of personal data aimed in particular at taking into account the provisions of Directive (EU) 2016/680 of 27 April 2016 referred to above, that the draft

decree which is submitted to it must be examined with regard to these provisions, and more particularly articles 87 and following of the law of January 6, 1978 as amended. The Commission notes in this regard that a data protection impact assessment (DPIA) was sent to it.

Reminder of the processing implemented within the framework of the system provided for in article 706-102-1 of the CPP and presentation of the main changes envisaged

The Commission recalls that the capture of computer data in the context of judicial information relating to offenses of delinquency and organized crime was introduced in Articles 706-102-1 et seq. of the CPP by Law No. 2011-267 of 14 March 2011 referred to above. The scope of this capture was then extended by law no. 2014-1353 of November 13, 2014 reinforcing the provisions relating to the fight against terrorism.

The processing implemented on the basis of article 706-102-1 of the CPP must thus make it possible to apprehend and collect computer data as they appear on the screen for the user (screenshots), as they are entered on the keyboard (keystrokes) or as they are received and transmitted by audiovisual peripherals (capture of sound and image received and transmitted during the use of a service online audiovisual).

The Commission notes that the draft decree submitted to it for opinion is intended to take account of changes to the aforementioned law no. 2016-731 of 3 June 2016, which firstly extended the scope of capture measures data stored in a computer system, and has, on the other hand, authorized the use of this technique, hitherto limited to the instruction, the flagrance or preliminary investigation with the authorization of the judge of freedoms and detention (JLD) at the request of the public prosecutor.

The Commission also notes that the Ministry also intends to take into account the changes made by the aforementioned Law No. 2019-222 of 23 March 2019, which harmonized the provisions applicable to special investigation techniques, namely the collection of technical data from connection, sound system and image capture as well as computer data capture.

In addition to the aforementioned changes, the Commission notes that the other conditions for implementing these processing operations remain unchanged.

On the purpose of the processing

Article 1 of the draft decree provides that the processing envisaged allows, under the authority and control of the judge of freedoms and detention or the investigating judge, the collection, recording and storage of computer data captured according

to the procedures set out in articles 706-95-11 et seq. and 706-102-1 et seq. of the Code of Criminal Procedure.

In general, the Commission observes that the scope of these devices, as well as the data that may be the subject of such recordings, have been the subject of constant and significant expansion in recent years. It notes that the investigation methods thus employed, which are particularly intrusive in that they lead to the collection of a large volume of data, are liable to seriously infringe respect for the privacy of the persons concerned. in question on the one hand, and third parties on the other.

It considers that the implementation of these systems must be accompanied by strong guarantees to ensure that the data thus captured, collected without the knowledge of the persons concerned, on an increasingly large number of individuals, does not relate no excessive interference with the fundamental rights and freedoms of the persons concerned.

Beyond the particularly intrusive nature, by nature, of these capture devices, the Commission notes that they have been the subject of a specific legislative framework, as have the methods of using the data collected in this context and the procedural and technical guarantees that must surround their implementation.

In this respect, it notes that Article 5 of the aforementioned law of June 3, 2016 widened the scope of these recordings, hitherto limited by Article 706-102-1 of the CPP to data as they appear. displayed on a screen for the user of an automated data processing system, as he enters it there by entering characters or as it is received and transmitted by peripherals, to the information as it is stored in a computer system.

In the same way, article 5 of the aforementioned law of June 3, 2016 also extended the use of this technique to the scope of the flagrance investigation and the preliminary investigation with the authorization of the judge of freedoms and detention in the request of the public prosecutor, provided that the investigation relates to offenses relating to organized crime and delinquency in application of articles 706-73 and 706-73-1 of the CPP. While the Commission notes that the decree of December 18, 2015 has been amended to take this into account, this change does not call for any particular comments on its part.

In this context, the Commission considers that the purpose pursued by the processing envisaged within the framework of the aforementioned provisions of the CPP is legitimate, in accordance with article 4-2° of the law of January 6, 1978 as amended.

On the nature of the data collected and processed

As a preliminary point, and given the nature of the systems intended to be implemented, the Commission notes that it is by definition difficult to draw up an exhaustive list of the data that can be collected insofar as all the information such as the user will enter them on his keyboard, view them on his screen, pronounce them or hear them via an audiovisual device or such as

they will be stored in a computer system, are likely to be collected, indiscriminately. It also notes that it is only after the capture that they are used with a view to their transcription in a report for the only data useful for the manifestation of the truth.

Firstly, the Commission notes that Article 706-95-18 of the CPP provides that the judicial police officer or the judicial police agent acting under his responsibility describes or transcribes, in a report which is submitted to the file, the recorded data which are useful for the manifestation of the truth. No footage relating to private life unrelated to the offenses referred to in the orders authorizing the measure may be kept in the file of the proceedings. It recalls in this respect that particular attention must be paid to the strictly necessary nature of the data recorded.

Secondly, and without calling into question the technical and operational constraints linked to the implementation of this type of system, the Commission recalls that article 35 of the amended law of 6 January 1978 provides for the obligation to mention , in the regulatory act establishing a processing operation under Article 31 of the same law, the categories of personal data recorded in the processing. It requests that the draft decree be supplemented on this point in accordance with the aforementioned provisions.

Having made these general observations, the Commission notes that the purpose of Article 2 of the draft decree is to allow the capture of data as stored in a computer system.

It takes note of the clarifications provided by the Ministry according to which this extension will concern all the data of a computer system, without distinction and that as such, information recorded on a hard disk, on e-mails which have not been opened by the user or even on the entirety of a file which has only been partially viewed by the person for whom it is intended.

Although the Commission does not call into question the very principle of capturing this data, as regulated by the legislator, it nevertheless intends to recall the observations made in its deliberation No. 2015-109 referred to above, more particularly with regard to the capture of data relating to an individual in relation to the person in question as well as that relating to a system not belonging to or not being used by the person concerned by the measure.

In this respect, it emphasizes that the draft decree mentions that all the data collected may be recorded, without it being expressly specified that data relating to the user of the information system, as well as to the people with whom he is in contact. Given the volume of data likely to be collected, and relating more particularly to third parties, it requests that the draft decree be clarified on this point.

In any case, the Commission takes note of the guarantees surrounding the implementation of these capture devices. It notes in

this respect that the processing operations governed by the draft decree are not subject to any linking or interconnection with other files.

In the same way, it acknowledges that remote control of the computer system is excluded (for example, the forced triggering of the webcam), and that if images as well as sounds may be collected, no facial or voice recognition mechanism or behavioral analysis of keystroke dynamics will not be implemented. The Commission recalls that if such techniques were to be developed in the future, it must be contacted under the conditions provided for in Article 33 of the amended law of January 6, 1978.

On the data retention period

While the Commission notes that the Ministry does not intend to make any changes to the retention period of the data, it emphasizes that the information recorded in the processing is kept until the investigation is closed and it is transmitted to the judicial authority. .

In this regard, it draws the Ministry's attention to the procedures for storing and accessing the recordings of data which were considered, at the time of transcription, to be unrelated to the investigation in progress, as well as data captured on a information system not belonging to the person in question. The Commission considers that, in these cases, specific measures will have to be implemented in order to guarantee their confidentiality. It also recalls that strict control must be exercised over their access.

Article 6 of the draft decree provides that any operation of collection, modification, consultation, transfer and deletion of personal data and information is subject to recording including the identification of the author, the date, time and nature of the transaction. This information is kept for a period of six years, which does not call for any particular comment from the Commission.

On the recipients

Article 4 of the draft decree provides that the agents of the tax services authorized to carry out judicial investigations in application of article 28-2 of the code of criminal procedure can access the data recorded in the processing.

The Commission notes that these agents are empowered to carry out investigations at the request of the public prosecutor or on the request of the investigating judge, thus conferring on them judicial police powers with regard to offenses falling within the scope of the provisions projected.

Given these elements, it considers that these agents are legitimate to access the data recorded in the processing operations

implemented, in compliance with the principle of the need to know and for the exclusive needs of the procedure in the context of which the capture operation has been authorized.

The aforementioned article 4 provides that the qualified personalities in charge of the control of the design work and the operations of implementation of the technical devices also have access to the information mentioned in article 6.

The Commission notes that Article 7 of the Order of 9 May 2018 creating the national technical service for judicial recording provides that the design work and operations to implement the judicial recording tools mentioned in Article 2 are placed under the control of two qualified personalities, respectively designated by the Minister of the Interior and the Minister of Justice, for a renewable period of five years. It also specifies that these persons may request the communication by the service of any information necessary for the exercise of their control mission.

The Commission acknowledges that only the traceability data will be accessible to them for the purpose of carrying out their control mission.

Without calling into question the need for these personalities to have communication of the traceability data recorded in the processing implemented, it notes that the aforementioned decree of 9 May 2018 seems to provide for a one-off communication, at their request, of this data. In this context and in the state of the information brought to its attention, the Commission recommends that these personalities only be made recipients of this category of data. It takes note of the commitment of the ministry to modify the draft decree in this sense as well as the DPIA transmitted.

On the rights of data subjects

Article 7 of the draft decree provides that the right of opposition provided for in article 110 of the law of January 6, 1978 referred to above does not apply to this processing. The aforementioned article also specifies that in accordance with articles 104 to 106 of the same law, the rights of information, access, rectification and erasure of the data mentioned in article 2 are exercised directly with the Ministry of the interior.

The Commission notes that people will be informed via the publication of the regulatory act as well as via the website of the Ministry of the Interior. It also notes that the exercise of all of these rights may be subject to restrictions, in order to avoid hampering investigations, research or administrative or judicial proceedings, or to protect public safety and security national, pursuant to 2° and 3° of II and III of article 107 of the law of January 6, 1978 as amended. Given the purpose of the processing, the limitation of these rights, which are exercised in such a case with the Commission under the conditions

provided for in Article 108 of this same law, does not call for any particular observation.

On security measures

The captured data processing system materializes by the discrete insertion of a logic load on the equipment of the targeted individual. Once activated, the software allows all the data present on the targeted medium to be sent to the police.

The Commission notes that the data to be collected are enriched by a signature and by an event log. It notes that then, before transfer, the data collected, accompanied by their event logs, are encrypted, using a public algorithm reputed to be strong, which does not call for comments.

It acknowledges that in order to consult the data, authorized personnel must connect to the data storage space via an encrypted connection of the VPN type. In addition, authorized personnel must authenticate themselves in a strong way, using a dongle and a password that must contain at least ten (10) characters including one special character, subject to an account blocking rule. after three unsuccessful attempts and having a validity period equal to the investigation time. The administrators, in charge of administering rights and providing level 2 support, must access the platform using an SSH connection subject to a password and then authenticate using a Smartcard. These elements call for no comments.

The Commission notes that the aforementioned administrators are the only ones authorized to issue passwords and to declare the right holders authorized to access the storage spaces (data containers), the end users having one password per case. In this regard, it encourages the ministry to implement a strong organization for managing passwords issued by administrators.

Finally, it notes that the ministry indicates that currently, no protection against non-human sources of risk (natural disasters for example), does not exist, the second site allowing the backup of the data not being chosen at the present time. . It notes that the ministry plans to use a backup site for backups by 2020.

The Commission considers that the security measures comply with the security requirement provided for in article 99 of the amended law of 6 January 1978. However, it recalls that this obligation requires the updating of security measures with regard to the regular reassessment of risks. In this respect, it recalls that specific attention should be paid to the reassessment of security measures in the context of the update of the impact analysis.

For the President:

Deputy Vice-President,

S. Lambremon