Deliberation 2021-071 of June 24, 2021Commission Nationale de l'Informatique et des LibertésNature of the deliberation: OpinionLegal status: In force Date of publication on Légifrance: Friday December 31, 2021NOR: CNIX2138803VDeliberation n° 2021-071 of June 24, 2021 providing an opinion on a draft decree authorizing the implementation of automated processing of personal data relating to breaches of automated data processing systems called "MISP-PJ" (request for opinion no. 20018973)

The National Commission for Computing and Liberties,Request by the Ministry of the Interior of a request for an opinion concerning a draft order authorizing the implementation of automated processing of personal data relating to attacks automated data processing systems called MISP-PJ;

Considering the modified law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms, in particular its article 31-I; After having heard the report of Mrs Sophie LAMBREMON, commissioner, and the observations of Mr. Benjamin TOUZANNE, Government Commissioner, Issues the following opinion: The Commission has been seized by the Ministry of the Interior, on the basis of article 31 of the law of January 6, 1978 as amended, of a request for an opinion concerning a draft decree authorizing the implementation of automated processing of personal data relating to breaches of automated data processing systems called MISP-PJ.

The Malware Information Sharing Platform - Judicial Police processing, hereinafter MISP-PJ , implemented by the General Directorate of the National Police of the Ministry of the Interior, aims to centralize the information contained in the legal proceedings in terms of attacks to automated data processing systems, as well as to facilitate the identification of the perpetrator of an offense and the corresponding investigations by cross-checking and analyzing this information.

It is fed by technical data from, on the one hand, the software for drafting legal proceedings of the national police (LRPPN) and the national gendarmerie (LRPGN) and, on the other hand, the processing of information collection techniques relating to security incidents on networks and information systems implemented by the computer attack alert and response center of the judicial police (CSIRT-PJ).

The Commission observes that the multiplication of cybersecurity-related risks and the growing sophistication of attackers' means require an adaptation of the tools available to national police and gendarmerie services. The diversity of the targets and the origin of the attacks can justify the search for connections between different situations. In general, the Commission welcomes this project which will contribute to a more effective fight against cybercrime.

Insofar as the purposes pursued by the processing enable the prevention, investigation, observation or prosecution of criminal offences, the Commission considers that it comes under the provisions of Titles I and III of the law of 6 January 1978 as amended. the purposes of the processing Article 1 of the draft decree provides that the purposes of the MISP-PJ processing are:

- on the one hand, to centralise, at the national level, the information contained in the legal proceedings opened in the national police and gendarmerie services with regard to breaches of the automated data processing system;
- on the other hand, to increase the effectiveness of the investigations by cross-checking and analyzing the information collected. the effectiveness of the investigations can be continued. It takes note that the ministry has modified article 1 of the draft order accordingly.

The MISP-PJ processing thus aims to make it possible to cross-check technical elements (or indicators of compromise) collected in the various legal proceedings. The cross-checks will be carried out automatically within the MISP-PJ application itself, which plans to signal when several files share an identical technical indicator. They will allow investigators to establish links between certain breaches and thus facilitate their investigations. The Commission notes that the results of the analyzes of these cross-checks and the results of the investigation will not be recorded in the MISP-PJ processing but in the judicial file.

With regard to processing covered by Directive (EU) 2016/680 of the European Parliament and of the Council of April 27, 2016, known as the Police/Justice Directive, Article 90 of the amended Law of January 6, 1978 provides that if the processing is likely to create a high risk for the rights and freedoms of natural persons, the data controller carries out an impact analysis relating to the protection of personal data (AIPD). If the processing is carried out on behalf of the State, this DPIA is sent to the Commission with the request for an opinion provided for in Article 33.

The ministry considers, in agreement with the ministerial delegate for data protection, whose opinion was sent to the Commission in the context of this request for an opinion, that, insofar as the MISP-PJ processing does not is not likely to create a high risk for the rights and freedoms of individuals, the performance of a DPIA is not necessary.

However, the Commission recalls that carrying out a DPIA is recommended even when it is not mandatory, in particular with regard to the purposes pursued by the processing and its scope. In particular, a DPIA would allow the Ministry to assess whether new risks relating to the persons concerned and linked to the fact of centralizing information must be taken into account as well as to monitor the evolution of these risks as the power increases. of the device.On the nature of the data

processedArticle 2 of the draft decree provides for the collection of personal data and information concerning the victims (legal or natural persons), the facts and the perpetrator of the attack , or investigation services accessing processing.

Article 2 of the draft decree provides that the following personal data and information may be collected as data and information relating to the perpetrator of the attack: email addresses, IP addresses, pseudonyms, social media profile name(s) or identifiers, domain name(s), port number, ransom demand email, ransom note, encrypted file data and file signature, wallet address of virtual currency.

In this regard, the Ministry specified that in addition to data from the ongoing legal proceedings, the MISP-PJ processing may be fed by technical data from open sources such as articles from antivirus companies and companies cybersecurity services working on families of ransomware or other malware.

The Commission considers that particular vigilance must be paid to the collection of data via open sources, in order to ensure that only the data strictly necessary for the purposes pursued by the processing are processed and recorded. In this regard, the Commission notes that the production of a DPIA would enable the Ministry to identify the appropriate security measures to avoid too broad a collection of data from open sources.On the retention period of dataArticle 3 of the draft of the decree provides that personal data and information are kept for a period of six years from their recording.

The Commission takes note of the information provided by the Ministry according to which such a duration is justified, on the one hand, by the fact that the perpetrators of the offenses referred to can reuse the same indicators of compromise several times over long periods and, on the other hand, on the other hand, by the fact that this duration corresponds to the limitation period in tort.

The Commission notes that the data retention period is not modulated according to the legal action taken. The ministry clarified in this respect that the legal consequences are not recorded in the MISP-PJ processing.

The Commission points out that the data retention period cannot be fixed, in principle, with regard to the sole limitation period for public action, without consideration of the purposes for which they are processed, and in compliance with the provisions of the article 4-5° of the modified law of January 6, 1978. It emphasizes the need to ensure that only the data strictly necessary for the purposes pursued by the processing are recorded, in particular by deleting the reports and complaints whose analysis will have made it possible to determine that they do not relate to breaches of the automated processing of data or by deleting reports and complaints that would not have triggered the opening of legal proceedings or would have been dismissed after

investigation.

The Commission also notes that a quarterly verification is carried out, during which a statement of the data whose retention exceeds the prescribed period is established. The data concerned is then deleted manually by persons with administrator rights. The Commission nevertheless recommends the implementation of automated deletion to ensure data retention does not exceed the established retention period. access the data and information of the processing or be the recipients, by reason of their attributions and within the limit of the need to know. The list of buyers does not call for comments from the Commission.

In particular, the recipients of personal data and processing information may be international cooperation bodies in the field of judicial police and foreign police services, which present, in accordance with the requirements of Article L. 235-1 of the Code of internal security a sufficient level of protection of the privacy, freedoms and fundamental rights of individuals with regard to the processing to which these data are subject or may be subject.

The same article provides that the national police and gendarmerie services may receive data contained in the processing operations managed by international cooperation organizations in the field of judicial police or foreign police services within the framework of the commitments provided for in this article. The Commission notes that only technical data transmitted in the context of a request for mutual legal assistance or a request for international cooperation (MLAT) will be recorded in the MISP-PJ processing. These data must correspond to the data described in article 2 of the draft decree.

In general, the Commission recalls that the transfer of personal data to States not belonging to the European Union or to recipients established in States not belonging to the European Union must be carried out in the compliance with the provisions of articles 112 to 114 of the law of January 6, 1978 as amended. On links The Ministry plans to link the MISP-PJ processing on the one hand with the software for writing the LRPPN and LRPGN procedures and, on the other hand, on the other hand with the collection of technical information relating to security incidents on the networks and information systems implemented by the CSIRT-PJ. This processing will feed the MISP-PJ processing, by means of manual reconciliations, with the technical data detailed in article 2 of the draft order.

The Commission considers that these connections are part of the purposes pursued by the MISP-PJ processing, namely the strengthening of the effectiveness of investigations into breaches of the automated data processing system by cross-checking and analyzing information collected.

It notes that, the CSIRT-PJ implements a processing of data and information relating to malicious software storing data relating

to security incidents detected via open sources or transmitted by partner organizations. According to the Ministry, the connection with the MISP-PJ processing should make it possible to contextualize the survey data thanks to this additional data. The Commission notes that the data recorded in the MISP-PJ processing resulting from the processing implemented by the CSIRT-PJ will be exclusively IP addresses of command servers or machines involved in the security incidents, e-mails and addresses of cyber-currencies and pseudonyms used during attacks. On data security and traceability of actions With regard to the security elements implemented to regulate the processing, the Commission recommends the drafting of a DPIA specifying the solutions techniques deployed to cover the risks associated with the data processed. As this DPIA was not deemed necessary by the Ministry with regard to the characteristics of the processing, the Commission cannot comment in depth on these aspects.

The Commission also recalls that the collection in one and the same place of the data listed below and their use in the context of legal proceedings may present risks in the event of loss of confidentiality. Indeed, the reconciled data, such as information relating to the author of the attack (IP addresses and port numbers, e-mail addresses used in the context of the attack, identifiers, pseudonyms, names of profiles on social networks, domain names or ransom demand email addresses) are elements whose processing requires an adequate level of security.

The ministry also specifies that the data contained in the processing will be recorded manually. It specifies that these are technical data resulting, on the one hand, from software for drafting legal proceedings LRPPN and LRPGN and, on the other hand, from the processing of the collection of technical information relating to security incidents on the networks and information systems implemented by the CSIRT-PJ. In this respect, the Commission wonders about the risks induced by manual recording and about the technical and organizational guarantees making it possible to ensure the quality of the data thus recorded in the MISP-PJ processing, as well as the integrity of this data in time. In this respect, it recommends adopting automatic import procedures.

The ministry does not specify the backup or partitioning solutions that will make it possible to limit the loss of confidentiality or integrity as well as the conservation over time of the data processed. However, he specifies that the solution will be deployed on his intranet.

The Commission retains in this regard that encryption of the processing access flow will be implemented and that access will be managed through authentication by identifier/password. Consequently, it recalls the need to implement authorization

management procedures to limit access to the sole right to know and that this procedure must take into account a regular review of the access thus granted.

With regard to data access controls, the Commission recalls that the authentication of persons authorized to access processed data must comply with Article 99 of the amended law of 6 January 1978, as clarified by its deliberation no. 2017-012 of January 19, 2017 adopting a recommendation on passwords.

Finally, concerning traceability, the ministry specifies that traceability will be implemented within the processing to cover all the operations carried out on it. With regard to their conservation, the ministry specifies that conservation for a period of 6 years will be carried out. The Commission recalls that it is not possible to justify the retention period of traceability data for the sole duration of the limitation period for criminal offenses related to the misuse of processing data by those who access it. It considers, in the present case, that keeping the traces for a period of three years could be considered justified. It recalls, in any case, that this should be accompanied by an automated alert management system allowing the detection of malicious use of the deployed solution.

The president,

M. L. Denis