Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI

Courtesy translation: *in the event of any inconsistencies between the French version and this English courtesy translation, please note that the French version shall prevail and have legal validity.*

The *Commission nationale de l'Informatique et des Libertés* (CNIL - French Data Protection Authority), met in its Restricted Committee consisting of Mr Alexandre LINDEN, Chair, Mr Philippe-Pierre CABOURDIN, Vice Chair, Ms Anne DEBET, Mr Bertrand du MARAIS, and Mr Alain DRU, members;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the free movement of such data;

Having regard to amended French Data Protection Act No. 78-17 of 6 January 1978, in particular Articles 20 *et seq.*;

Having regard to Decree No. 2019-536 of 29 May 2019 implementing French Data Protection Act No. 78-17 of 6 January 1978;

Having regard to Deliberation No. 2013-175 of 4 July 2013 adopting the CNIL's internal rules of procedure;

Having regard to the CNIL Chair's Decision No. 2020-116C of 26 August 2020 to instruct the Secretary General to verify or have a third party verify the processing implemented by CLEARVIEW AI;

Having regard to Decision No. MED 2021-134 of 26 November 2021 serving an order on CLEARVIEW AI;

Having regard to the CNIL Chair's decision appointing a rapporteur before the Restricted Committee of 2 June 2022;

Having regard to the report of Claude CASTELLUCCIA, the commissioner rapporteur, notified to CLEARVIEW AI on 14 July 2022;

Having regard to the oral observations made at the Restricted Committee session on 13 October 2022;

Having regard to the other documents in the case file;

Mr Claude CASTELLUCCIA, Commissioner, whose report was read, was present at the Restricted Committee session.

Duly convened, by letter delivered against signature on 20 September 2022, CLEARVIEW AI was not represented at the Restricted Committee session.

After having deliberated, the Restricted Committee adopted the following decision:

I. Facts and proceedings

1. CLEARVIEW AI (hereinafter "the company" or "Clearview AI"), established in the United States, was founded in 2017. It has developed facial recognition software, whose database is based on the extraction of images publicly accessible on the Internet, which allows an individual to be identified using a representative photograph.

A. The origin of the proceedings

2. Between May and December 2020, the *Commission nationale de l'informatique et des libertés* (hereinafter the "CNIL") received several complaints relating to the difficulties encountered by the complainants in exercising their rights of access and erasure with the company.

3. Pursuant to the CNIL Chair's Decision No. 2020-116C of 26 August 2020, a Commission delegation carried out a documentary investigation, by sending a questionnaire on 27 October 2020, to which the company replied by letter dated 27 November 2020. This questionnaire concerned the different processing implemented by the company, the organisations which use the company's services (current or former) having their principal place of business in France or within the European Union, as well as complaint No. […] and No. […].

4. On 27 May 2021, the CNIL received a complaint from Privacy International (Referral No. […]).

5. As part of the mutual assistance provided for in Article 61 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the "GDPR" or the "Regulation"), the CNIL has been provided with useful information by its European counterparts.

B. The order sent to CLEARVIEW AI by the CNIL Chair

6. By Decision No. 2021-134 of 26 November 2021, the CNIL Chair issued an order to CLEARVIEW AI to comply with the provisions of Articles 6, 12, 15 and 17 of the GDPR within two months.

7. In the absence of a response to the CNIL Chair's order and two reminders, on 2 June 2022, the Commission Chair appointed Mr Claude CASTELLUCCIA as rapporteur, on the basis of Article 22 of the amended French Data Protection Act of 6 January 1978.

8. At the end of his investigation, on 14 July 2022, the rapporteur arranged for the company to be notified of a report detailing the breaches of the GDPR that he considered established in this case.

9. The company did not produce any written observations in response to this report and the file was included on the agenda of the Restricted Committee session of 13 October 2022.

10. The rapporteur presented oral observations at the Restricted Committee session.

C. The processing in question

11. It emerges from the information transmitted within the framework of cooperation between supervisory authorities, publicly accessible information, and complaints received by the CNIL that the company uses its own technology to index freely accessible web pages. It collects all images in which faces appear, on millions of websites. Photographs are thus extracted from social networks (e.g., Twitter or Facebook), professional websites containing photographs of their employees, blogs, and any websites on which photographs of individuals are publicly accessible. Images are also extracted from videos available online, e.g., on the website www.youtube.com. This collection relates to images of adults and minors, with no filter being applied in this regard. Only a few hundred URLs, associated with "*adult*" sites with some of the largest audiences, are blocked and excluded from collection.

12. The collection of these images on social networks covers all images accessible at the time of collection to an individual who is not connected to the network in question. In addition to social media, the collection concerns all images accessible to a search engine at the time of collection. Thus, the company has collected over twenty billion images worldwide.

13. From each photograph collected, the company calculates a biometric template. This way, a unique mathematical hash specific to the face as it appears in the photograph (based on the points of the face) is generated. Billions of images are then recorded in a database in a searchable form (using the mathematical hash).

14. The company sells access to an online platform featuring a search engine. This tool is used by uploading a picture of a face. From that photograph, the tool calculates the mathematical hash corresponding to it and carries out a search for photographs in the database linked to similar mathematical hash. The software produces a search result, composed of photographs, which is associated with the URL of the web page from which the photographs were extracted (social network, press article, blog, etc.). This search result thus compiles all the images collected by the company about an individual, as well as the context in which these images are online, such as, for example, a social network account or a press article.

15. The purpose of this processing is to uniquely identify the individual from a photograph of the individual. It is therefore a facial recognition device.

16. The company describes the service it offers as "*a research tool used by law enforcement authorities to identify perpetrators and victims of offences*" using a photograph. It is indicated on its website that, for example, this tool enables "*analysts*" to conduct a search by uploading crime scene images to compare them to those that are publicly available. According to the company, this allows law enforcement to use this tool to identify an individual for whom they have an image (e.g., from a CCTV recording) but do not know the identity.

17. It should be noted that the processing operations carried out by the company in order to collect data and create a database, which a search engine accesses in order to provide a result, are analysed globally, in view of their common purpose, which is to market a search engine based on facial recognition (hereinafter, "the processing in question").

II. Reasons for the decision

A. On the applicability of the GDPR

18. Pursuant to Article 3(2) GDPR: "*This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: […] b) the monitoring of their behaviour as far as their behaviour takes place within the Union.*". The Restricted Committee points out that the GDPR does not require, in order to be applicable, that the purpose of the processing be the monitoring of behaviour, but that it is "*related*" to the monitoring of the behaviour of individuals residing in Europe.

19. Recital 24 GDPR states in this respect that "*The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes*".

20. By way of clarification, in its Guidelines 3/2018 on the territorial scope of the GDPR in their version of 12 November 2019, the European Data Protection Board (hereinafter "the EDPB") states that, "*As opposed to the provision of Article 3(2)(a), neither Article 3(2)(b) nor Recital 24 expressly introduce a necessary degree of 'intention to target' on the part of the data controller or processor to determine whether the monitoring activity would trigger the application of the GDPR to the processing activities. However, the use of the word 'monitoring' implies that the controller has a specific purpose in mind for the collection and subsequent reuse of the relevant data about an individual's behaviour within the EU. The EDPB does not consider that any online collection or analysis of personal data of individuals in the EU would automatically count as 'monitoring'. It will be necessary to consider the controller's purpose for processing the data and, in particular, any subsequent behavioural analysis or profiling techniques involving that data. The EDPB takes into account the wording of Recital 24, which indicates that to determine whether processing involves monitoring of a data subject behaviour, the tracking of natural persons on the Internet, including the potential subsequent use of profiling techniques, is a key consideration*".

21. To the extent that the company is not established in the European Union, it is therefore necessary, in order for the GDPR to apply to the processing in question, to determine whether the company processes personal data relating to data subjects in the territory of the European Union and whether this processing is linked to the monitoring of the behaviour of those individuals.

22. **Firstly**, it stands out from the company's privacy policy that it collects in particular:
    - photographs publicly accessible on the Internet;
    - information that can be extracted from such photographs, such as geolocation metadata that the photograph may contain;
    - information derived from the facial appearance of people in such photographs.

23. These three categories of data constitute personal data of the individual whose face appears in the photograph in question. Indeed, the concept of personal data is defined in the GDPR as "*any information relating to an identified or identifiable natural person […]*", this identification may relate in particular "*to one or more factors specific to the physical, [...] identity of that natural person*". The image of the individual photographed or filmed constitutes personal data when the individual is identifiable, i.e. they can be recognised (see CJEU, fourth chamber, 11 December 2014, Rynes, C-212/13, point 22 and CJEU, second chamber, 14 February 2019, F.K., C-345/17). In addition, this image can be compared (by automated or non-automated means) with an image held elsewhere and attached to an identified individual so that the identity of that individual can be deduced.

24. Furthermore, the company processes biometric data associated with such images. Personal data resulting from specific technical processing, relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images, constitutes biometric data, within the meaning of Article 4.1.14 of the Regulation. This data is generally referred to as "biometric templates" and constitutes data separate from source images (see CNIL, SP, 25 June 2020, Opinion on draft decree, PASP, No. 2020-064, published).

25. In addition, the images collected concern individuals located in the European Union. Indeed, such collection is not geographically limited to the US territory on which the company is established, since such data is collected on the Internet, particularly from global social networks.

26. Consequently, the company processes personal data of natural persons located in the European Union and, in particular, in France.

27. **Secondly**, it is necessary to verify whether the processing activity in question can be considered as "related to the monitoring of behaviour" of the data subjects within the meaning of Article 3 GDPR. It should be noted that the GDPR does not only apply to processing whose primary purpose is to monitor the behaviour of an individual residing in the European Union, but to all processing operations which are "related" to such monitoring, i.e. which are carried out by means of or in connection with operations monitoring individuals residing in Europe.

28. In accordance with Recital 24 of the GDPR, the concept of monitoring on the Internet includes the possible subsequent use of personal data processing techniques consisting of profiling a natural person. Profiling is defined in Article 4.1.4 GDPR as "*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*".

29. Firstly, the processing in question leads to the creation of a behavioural profile of all the individuals whose data is collected.

30. It emerges from the information transmitted within the framework of cooperation between supervisory authorities that the tool in question makes it possible to generate, from an image and subject to a margin of technical error, a search result containing all the photographs collected by the company, on which appears a face with a biometric template sufficiently close to the face appearing on the photograph used for the search.

31. The profile thus created, relating to an individual, is composed of photographs but also the URL of all the web pages on which those photographs are located. However, linking photographs and the context in which they are presented on a website makes it possible to gather many pieces of information about an individual, their habits or preferences. With regard in particular to social media, a photograph and the original URL of that photograph are highly likely to identify the account of the data subject. The photographs may also have been posted online to illustrate a press or blog article, which is therefore likely to contain precise information about the data subject and thus elements relating to their behaviour.

32. In addition, the search result displayed may also include metadata, such as geolocation metadata, which is likely to be contained in the photographs or videos. This data makes it possible to supplement an individual's profile.

33. Furthermore, such a search result also makes it possible to identify a person's behaviour on the Internet, by analysing the information that this individual has chosen to put online as well as its context. Indeed, the posting of photographs in itself constitutes behaviour of the data subject, reflecting choices on the level of exposure that they wish to give to elements of their private or professional life.

34. Therefore, it should be considered that the search result associated with a photograph must be qualified as a behavioural profile of the data subject insofar as it contains numerous pieces of information about that individual, and in particular their behaviour, or allows access to them. The processing in question thus constitutes profiling within the meaning of Article 4.1.4 in that it makes it possible to assess certain personal aspects relating to a natural person, in particular to analyse aspects concerning their personal preferences, interests, behaviour or location.

35. Finally, it should be noted that such a behavioural profile mainly concerns behaviour that took place within the European Union. Indeed, insofar as they are individuals resident in the EU, they carry out most of their online activity in the EU. In addition, to the extent that such individuals are resident in the EU, most of the information relating to their private and professional life relates to behaviour that takes place in the EU.

36. Even assuming that the purpose itself of the processing is not behavioural monitoring, the means used to enable the company's biometric identification system involve the creation of such a profile, and the processing must be regarded as "*linked to the monitoring of the behaviour*" of the data subjects.

37. Secondly, the automated data processing enabling the creation of such a behavioural profile and its availability to individuals who make queries in the company's search engine must be qualified as monitoring on the Internet.

38. Indeed, the very purpose of the tool marketed by Clearview AI is to be able to identify and collect certain information relating to an individual. The implementation of the various stages of the processing described above, and particularly biometric techniques making it possible to distinguish an individual, lead to the creation of a behavioural profile. However, such a profile is created in response to a search conducted by an individual and relating to an individual appearing in a photograph.

39. In addition, the search can be renewed over time, which makes it possible to observe a change in the information about an individual, particularly if the results of the successive queries are compared. Indeed, since the database is updated regularly, successive searches make it possible to monitor the evolution of a profile over time.

40. Therefore, the fact that an ad hoc search makes it possible, at any time, to access an individual's profile as described above should be considered as monitoring the behaviour of individuals.

41. The Restricted Committee therefore considers that the processing carried out is linked to the monitoring of the behaviour of data subjects within the meaning of the provisions of Article 3.2.(b) GDPR and falls within the territorial scope of the GDPR.

42. It also follows from all of the above that Clearview AI, which defines the purposes and means of the processing, must be considered as the data controller with regard to the establishment of the database, which is then used to market its service.

B. On the competence of the CNIL and the lack of applicability of the one-stop-shop mechanism

43. Article 55.1 GDPR stipulates that "*each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State*".

44. Article 56.1 provides: "*Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.*"

45. Recital 122 GDPR states: "*Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. This should cover in particular the [...] processing carried out by a controller or processor not established in the Union when targeting data subjects residing on its territory. […]*"

46. It follows from a combined reading of Articles 55 and 56 GDPR that, in the event that a data controller established outside the European Union implements cross-border processing subject to the GDPR, but there is no principal place of business or sole establishment, the one-stop shop mechanism provided for in Article 56 GDPR is not intended to apply. Each national supervisory authority is therefore competent to monitor compliance with the GDPR in the territory of the Member State to which it belongs.

47. In this case, the company is established in the United States and has no establishment in the territory of a Member State of the European Union.

48. Consequently, the Restricted Committee considers that the one-stop shop mechanism does not apply and the CNIL is competent to ensure, on French territory, that the processing operations are carried out in accordance with the provisions of the GDPR.

C. On the breach of the obligation to have legal grounds for the processing carried out

49. Article 6 of the GDPR states that: "*Processing shall be lawful only if and to the extent that at least one of the following applies:*
(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

50. Recital 47 GDPR states that "*The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. […]*"

51. **The rapporteur** considers that the company has no legal grounds for the processing in question, in breach of Article 6 of the Regulation.

52. **The company** has not made any observations in defence.

53. **The Restricted Committee** notes that, to be lawful, the processing of personal data must therefore be based on one of the legal grounds referred to above.

54. It appears from the information transmitted within the framework of cooperation between supervisory authorities that the facial recognition software implemented by the company is based on the systematic and widespread collection, from millions of websites around the world, of images containing faces, using an exclusive technology to index freely accessible web pages.

55. The company then processes the data collected in order to create a database and enable the searching of photos in this database using another image.

56. Such processing is carried out by the company solely for commercial purposes, regardless of the fact that the search engine would be used by law enforcement in certain States.

57. As part of the investigations carried out by the CNIL, the company was questioned on the legal basis of that processing, within the meaning of Article 6 GDPR. The company did not provide any response on this point. The company's privacy policy, previously mentioned, also does not mention the legal basis for such processing.

58. It can be noted from the outset that the company has not obtained the data subjects' consent to the processing of their personal data.

59. Furthermore, the Restricted Committee notes that, given the nature of the processing in question, the legal bases provided for by the provisions of Article 6.1 (b), (c), (d) and (e), GDPR and related to the performance of a contract, the fulfilment of a legal obligation, the protection of the vital interests of the data subject or another natural person, and the performance of a task in the public interest, are not applicable in this case.

60. As regards the legal basis related to the legitimate interests pursued by the data controller, as provided for in Article 6. 1. (f) of the Regulation, it should be recalled that the "*publicly accessible*" nature of data does not affect the qualification of personal data and that there is no general authorisation to re-use and further process publicly available personal data, particularly without the knowledge of the data subjects.

61. By way of illustration, the Article 29 Working Party (called "WP29" now the EDPB), in its Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, noted in this respect that "*personal data, even if it has been made publicly available, continues to be considered as personal data*" and that "*its processing therefore continues to require appropriate safeguards*". While acknowledging that the fact that personal data is publicly available may be a relevant factor in concluding that there are legitimate interests, the EDPB then warned that this would only be the case "*if the publication was carried out with a reasonable expectation of further use of the data for certain purposes (e.g. for purposes of research or for purposes related to transparency and accountability).*"

62. Furthermore, in order for the data controller to be able to avail itself of these legal grounds, processing must be necessary for the purposes of the legitimate interests it pursues, unless the interests or the fundamental rights and freedoms of the data subjects take precedence.

63. Even if the company's interests were based on the economic interest it derives from the operation of the database in question, this interest should, however, be balanced against the interests or fundamental rights and freedoms of the data subjects, taking into account the reasonable expectations of the individuals based on their relationship with the data controller, in accordance with Article 6.1(f) GDPR, read in the light of Recital 47 and the aforementioned opinion on the notion of legitimate interest.

64. In this case, the processing is particularly intrusive: the company collects from a given individual a large number of photographic data, which is associated with other personal data likely to reveal various aspects of their private life. Based on that data, a biometric template is established, i.e., biometric data that can, if reliable, be used to uniquely identify an individual from a photograph of that individual: the holding of such data by a third party constitutes a

significant breach of privacy rights. Finally, this processing concerns an extremely high number of individuals.

65. Furthermore, it is necessary to determine in particular whether the data subjects could reasonably expect, at the time and in the context of the collection of personal data, that Clearview AI would process this personal data. In this respect, there is no relationship between the company and the data subjects. If they may reasonably expect third parties to access the photographs in question from time to time, the publicly accessible nature of the photographs is not sufficient to consider that the data subjects can reasonably expect their images to feed facial recognition software. Finally, the software operated by the company is not public and the vast majority of the data subjects are unaware of its existence.

66. It must therefore be considered that individuals who have published photographs of themselves on websites, or consent to such publication with another data controller, do not expect that they will be reused for the purposes pursued by the company, i.e., the creation of facial recognition software (which combines the image of an individual with a profile containing all the photographs in which they appear, the information those photographs contain as well as the websites on which they are located) and the marketing of this software to law enforcement authorities.

67. Therefore, with regard to all of these elements, the Restricted Committee considers that the breaching of individuals' privacy rights appears disproportionate in view of the interests of the data controller, in particular its commercial and financial interests. The legal basis of the company's legitimate interest cannot therefore be upheld.

68. Finally, the company did not respond to the requests made on this point in order No. MED 2021-134 of 26 November 2021. The Restricted Committee therefore considers that the company was not compliant on the expiry of the time limit set, nor subsequently.

69. **Consequently, the Restricted Committee considers that the company has no legal grounds for the processing in question, in breach of Article 6 of the Regulation.**

D. On the breach of the obligation to respect the right of access

70. Article 15 GDPR stipulates that: "*The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data […]*". This Article also provides for the different categories of information that the data controller must provide to the data subject in the event of a request for access.

71. Article 12 states that: "*The controller shall facilitate the exercise of data subject rights under Articles 15 to 22*".

72. **The rapporteur** accuses the company of not responding effectively to requests for access addressed to it and of not facilitating the exercise of the data subjects' right of access.

73. **The company** has not submitted any observations in defence.

74. **The Restricted Committee** notes that it follows from Referral No. […] that the complainant who submitted this referral asked the company for access to her data and to all the information

relating to such data within the meaning of Article 15.1, by electronic means. In fact, the complainant instructed a third party to make her request for access to the company. Clearview AI acknowledged receipt while inviting the complainant to use an online platform to exercise her request. More than two months after the initial request and three other e-mails sent by the contracted third party, the company requested the submission of a photograph and ID from the complainant and again invited the complainant to use an online platform to exercise her request. Four months after the initial request, following further exchanges relating to the transmission of ID and in the absence of a satisfactory response, the appointed third party sent a letter of formal notice to the company.

75. The Restricted Committee notes that the response given by the company to the request is, first of all, partial. Indeed, it only contains the result of the search in the tool marketed by the company, i.e., the images and the information associated with them. All the information provided for in Article 15.1 GDPR is therefore missing, since the company has merely provided a link to its privacy policy.

76. Secondly, the Restricted Committee considers that, by agreeing to respond to the complainant's request for access only after seven letters and more than four months after her initial request, and by requiring a copy of her ID when the complainant had already provided information to identify her and a photograph depicting her, Clearview AI did not facilitate the exercise of the complainant's rights.

77. Finally, it follows from the company's privacy policy that it limits the exercise of the right of access to the data collected in the twelve months preceding the request and restricts the exercise of this right to twice a year. However, the company's privacy policy does not specify the retention period of the data and it does not appear from the elements of the file that the retention period of the data in question would be limited to twelve months. Thus, the limitation on the right of access has no basis.

78. In addition, the Restricted Committee notes that the company did not respond to the injunctions formulated on this point in Order No. MED 2021-134 of 26 November 2021, allowing it to be established that the company would comply with them within the time limit of two months or in the future.

79. Consequently, the Restricted Committee considers, on the one hand, that the company breached its obligations by not providing a satisfactory response to the complainant and, on the other hand, that the company does not effectively respond to requests for access addressed to it and does not facilitate the exercise of the data subjects' right of access, in violation of Articles 12 and 15 of the Regulation.

E. On the breach of the obligation to respect the right to erasure

80. Article 17 GDPR provides: "*The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: […] the personal data have been unlawfully processed*".

81. **The rapporteur** considers that the company has disregarded a data subject's right to erasure by not responding to their request for erasure of their data.

82. **The company** has not submitted any observations in defence.

83. **The Restricted Committee** notes that it follows from Referral No. […] that the complainant who submitted this referral received no response from the company concerning the request for erasure of her data.

84. However, the Restricted Committee stresses that since the processing carried out cannot be based on any valid legal grounds in the light of European regulations, erasure was legally binding. The company should therefore have responded favourably to the complainant's request for erasure.

85. In addition, the Restricted Committee notes that the company did not respond to the injunctions formulated on this point in Order No. MED 2021-134 of 26 November 2021, allowing it to be established that the company would comply with them within the time limit of two months.

86. Consequently, the Restricted Committee holds that the company disregarded the complainant's right to erasure by not responding to her, in breach of Article 17 of the Regulation.

F. On the breach of the obligation to cooperate with the CNIL's departments

87. Article 31 GDPR states that "*The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks*".

88. **The rapporteur** accuses the company of not having responded satisfactorily to the CNIL's requests within the time limits set.

89. **The company** has not submitted any observations in defence.

90. **The Restricted Committee** notes that the company received an audit questionnaire from the Commission delegation, to which it only replied very partially.

91. The company then received an order dated 26 November 2021. This order contained various requests aimed at ensuring the compliance of the processing operations and the respect of individuals' rights.

92. The Restricted Committee stresses that the company did not respond to this order, nor to the reminder sent by the CNIL Chair on 3 March 2022, nor to the reminder sent by the Commission's departments on 4 April 2022.

93. Under these conditions, the Restricted Committee considers that these elements constitute a breach of the provisions of Article 31 of the Regulation since the company has not provided any response to the CNIL's requests.

III. On the sanction and publicity

94. Under Article 20 (III) of the amended French Data Protection Act of 6 January 1978, "*When the data controller or the processor fails to comply with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or this law, the CNIL Chair may also, if applicable, after sending the warning provided for in point I of this article or, where applicable, in addition to an order provided for in II, contact the Commission's Restricted Committee with a view to the announcement, after adversarial proceedings, of one or more of the following measures: [...]*

2. An injunction to make the processing compliant with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or this Act or to comply with the requests made by the data subject to exercise their rights, which may be accompanied, except in cases where the processing is implemented by the State, with a periodic penalty payment not exceeding €100,000 per day of delay from the date fixed by the Restricted Committee;

7. With the exception of cases where the processing is implemented by the State, an administrative fine may not exceed €10 million or, in the case of an undertaking, 2% of the total worldwide annual turnover of the preceding financial year, whichever is greater. In the cases mentioned in 5 and 6 of Article 83 of Regulation (EU) 2016/679 of 27 April 2016, these upper limits are increased, respectively, to €20 million and 4% of the said turnover. In determining the amount of the fine, the Restricted Committee shall take into account the criteria specified in the same article 83 […]".

A. On the issue of an administrative fine and its amount

95. Article 83 GDPR further states that "*each supervisory authority shall ensure that the administrative fines imposed […] are, in each individual case, effective, proportionate and dissuasive*", before specifying the elements to be taken into account when deciding whether to impose an administrative fine and to decide on the amount of that fine.

96. The Restricted Committee must therefore take into account, when determining the amount of the fine, criteria such as the number, nature and severity of the breaches, the degree of cooperation with the supervisory authority, the number of data subjects and the categories of personal data affected.

97. The Restricted Committee notes that the breaches committed are particularly serious, notably with regard to the infringement of the fundamental principles provided for by the GDPR, the number of data subjects concerned and the particularly intrusive nature of the processing in question.

98. The Restricted Committee therefore points out that the processing concerns more than twenty billion images as well as a considerable number of data subjects worldwide. There are therefore several million people in France whose faces appear on a photograph or video publicly accessible on the Internet, and in particular on a social media account, who are likely to be affected by this processing. As the database is also updated very regularly to integrate the newly available information, the number of these images and of these people is constantly evolving.

99. This massive processing is also particularly intrusive in that it collects a potentially very large amount of photographic data about a given individual, to which is related other personal data likely to reveal various aspects of their private life such as their tastes and preferences (e.g. in terms of leisure), political opinions or religious beliefs, expressed on social networks, blog posts or in press articles.

100. On the basis of this data, a biometric template, i.e. biometric data considered sensitive under Article 9 GDPR, is also established.

101. The Restricted Committee then notes the extreme severity of the breach of Article 6 GDPR. The company carries out this processing unlawfully since it has no legal basis for this purpose, no legitimate interest of the data controller or no consent of those concerned.

102. In addition, the company has clearly demonstrated that it does not wish to cooperate with the CNIL's departments. It only provided a very fragmented response to the audit questionnaire sent by the CNIL delegation and provided no response to the order from the Chair, despite several reminders.

103. Accordingly, the Restricted Committee considers that all of these breaches justify an administrative fine being imposed.

104. With regard to the amount of the fine, the Restricted Committee notes first of all that the breaches relating to Articles 6, 12, 15 and 17 of the GDPR are breaches of basic principles which, under Article 83 of the GDPR, may be subject to an administrative fine of up to €20,000,000 or up to 4% of the annual turnover, whichever is greater.

105. The Restricted Committee points out that, despite the CNIL's requests, the company has not provided any information relating to its turnover. It notes, however, that it emerges from journalistic sources that the company was valued at €130 million at the beginning of 2021.

106. In any event, the Restricted Committee considers that the extent of the processing in question, the severity of the breaches and the biometric nature of the personal data concerned, require that the administrative fine be particularly significant in order to be effective, dissuasive and proportionate.

107. In view of all these elements, the Restricted Committee considers that the issue of a fine of twenty million euros is justified.

B. On the issue of an injunction with a periodic penalty payment

108. **Firstly**, the Restricted Committee notes that the company has not provided any information that would tend to demonstrate its compliance with Articles 6, 12, 15 and 17 of the GDPR following the CNIL Chair's order of 26 November 2021. The company therefore continues to implement the processing in question unlawfully since it has no legal basis for this purpose. In addition, it provided no satisfactory response to the complainant's requests.

109. Consequently, since the breaches identified in this decision persist and in view of their degree of severity, the Restricted Committee considers it necessary to issue an injunction so that the company makes itself compliant with its obligations.

110. **Secondly**, the Restricted Committee points out that a periodic penalty payment is a financial penalty per day of delay to be paid by the data controller in the event of non-compliance with the injunction at the end of the stipulated time limit. Its imposition may therefore sometimes be necessary to ensure the compliance of the data controller within a certain period of time.

111. The Restricted Committee adds that for the purpose of preserving the comminatory function of this periodic penalty payment, its amount must be both proportionate to the severity of the alleged breaches but also adapted to the financial capacity of the data controller. It further notes that to determine this amount, account should also be taken of the fact that the breach to which the injunction relates, indirectly contributes to the profits generated by the data controller.

112. In the light of these two elements, the Restricted Committee considers it proportionate that a penalty amounting to €100,000 per day of delay and payable at the end of a two-month period be imposed.

C. On the publicity of the decision

113. The Restricted Committee considers that the publication of this Decision is justified in view of the severity of the breaches, the scope of the processing and the number of data subjects.

114. In particular, the Restricted Committee stresses that the publication of the decision to impose a sanction is necessary in order to inform the data subjects of the existence of this mechanism of which the vast majority of them will not be aware.

115. Finally, it considers that this measure is not disproportionate since the decision will no longer identify the company by name upon expiry of a two-year period following its publication.

FOR THESE REASONS

After having deliberated, the CNIL's Restricted Committee has decided to:

- **impose an administrative fine of €20,000,000 (twenty million euros) against CLEARVIEW AI;**

- **issue an injunction against CLEARVIEW AI** to not carry out the collection and processing of personal data relating to data subjects located on French territory, without legal grounds, as part of the operation of the facial recognition software that it markets, and to delete all the personal data of these individuals, in particular, the data of the complainant in question who requested erasure (complaint No. […]), after responding to the access requests already made by the individuals where applicable;

- **attach to the injunction a periodic penalty payment of one hundred thousand euros (€100,000) per day of delay at the end of a two-month period** following notification of this decision, with proof of compliance to be sent to the Restricted Committee within this period;

- **publish its decision on the CNIL and Légifrance websites, which will no longer identify the company at the end of a two-year period following its publication.**

The Chair

Alexandre Linden

This decision may be appealed before the French State Council within four months of its notification.