Decision n° MED 2021-134 of 1st November 2021 issuing an order to comply to the company CLEARVIEW AI

(No. MDMM211166)

This document is a courtesy translation of the official deliberation published on Legifrance.

In the event of any inconsistencies between the French version and this English courtesy translation, please note that the French version shall prevail.

The Chair of the Commission Nationale de l'Informatique et des Libertés (CNIL),

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 the amended French Data Protection Act No. 78-17 of 6 January 1978, particularly Article 20;

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 Decision No. 2013-175 of 4 July 2013 adopting the rules of procedure of CNIL (French Data Protection Agency);

Having regard to Decision No. 2020-116C of 26 August 2020 of CNIL's Chair to instruct the general secretary to carry out or have a third party carry out an assignment to verify the processing implemented by the company CLEARVIEW AI;

Having regard to Referrals No. 20012263, No. 20008376, No. 20022230 and No. 21010202;

Having regard to the documentary audit questionnaire dated 27 October 2020;

Having regard to the other documents in the file;

I. The procedure

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

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

Pursuant to decision No. 2020-116C of 26 August 2020 of the CNIL Chair, a CNIL 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 complaints No. 20008376 and No. 20012263.

On 27 May 2021, CNIL received a complaint from the organisation, Privacy International (Referral No. 21010202), concerning the company's facial recognition software and its use by law enforcement authorities.

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 "GDPR"), CNIL has been provided with useful information by several of its European counterparts.

II. Background

It emerges from the relevant information transmitted within the framework of cooperation between supervisory authorities, publicly accessible information, and complaints received by the Commission that the company uses its own technology to index freely accessible Internet 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 sites 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 largest audiences, are blocked and excluded from collection.

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 ten billion images.

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).

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 they were extracted (social network, press article, blog, etc.). This search result thus compiles all the images collected by the company about a person, as well as the context in which these images are online, such as, for example, the social network account or a press article.

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. 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.

III. On the applicability of the GDPR

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." (emphasis added).

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*" (emphasis added).

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*".

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

Firstly, it stands out from the company's privacy policy, attached as an appendix, that the company 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.

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 as soon as the individual is identifiable, i.e., they can be recognized. In addition, this image can be compared (by automated or non-automatic means) with an image held elsewhere and attached to an identified individual and the identity of that individual can be inferred. The company also processes biometric data associated with such images.

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 are collected on the Internet, particularly from global social networks. CNIL notes that, as part of its responses to the questionnaire sent by the investigation delegation, the company acknowledges processing personal data of European residents, particularly by asserting that it grants all access and opposition requests made by residents of the European Union. In particular, individuals located in France were concerned by the processing in question since the CNIL has received three complaints from by individuals residing in France concerning the difficulties encountered in exercising their rights of access and objection with the company.

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

Secondly, in order to establish whether the processing activity in question can be considered linked to the **monitoring of the behaviour of data subjects** within the meaning of Article 3 GDPR, it is necessary to determine whether the natural persons are monitored on the Internet.

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 GDPR as "*any form of automated processing of personal data consisting of using such personal data to assess certain personal aspects relating to a natural person*". It should also be pointed out that Article 3 GDPR does not require the processing to be carried out for the purpose of monitoring the behaviour of individuals but simply "linked" to it.

First of all, 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").

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

It appears from the relevant information, transmitted within the framework of the cooperation between the supervisory authorities, that the tool in question makes it possible to generate, using a photograph, a search result containing all the photographs with a biometric template sufficiently close to it. This search result includes all the photographs in which a person's face appears and which have been collected by the company, subject to a technical margin of error.

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 a person, 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 person concerned. 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.

In addition, the images may contain metadata, such as geolocation metadata, which are also included in the search result and supplement an individual's profile.

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 person concerned, reflecting choices on the level of exposure that they wish to give to elements of their private or professional life.

Therefore, it should be considered that the search result associated with a photograph should be qualified, at least in part, as a behavioural profile of the data subject insofar as it contains numerous pieces of information about that individual and in particular their behaviour. Even assuming that the purpose itself of the processing is not behavioural monitoring, the means used to enable Clearview's biometric identification system involve the creation of such a profile, and the processing can be regarded as "*linked to the monitoring of the behaviour*" of the data subjects.

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.

Indeed, the very purpose of the tool marketed by Clearview 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 an profile is created in response to a search conducted by an individual and relating to an individual appearing on a photograph.

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.

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.**

The processing thus carried out is therefore 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.

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

Article 55.1 GDPR provides 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*".

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."*

Recital 122 of the 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 […]*"

It stands out 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 central administration or establishment with decision-making powers as to its purposes and resources, 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.

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

Consequently, the one-stop shop mechanism is not applicable and CNIL is competent to ensure, on French territory, that the processing is implemented in accordance with the provisions of the GDPR.

V. On breaches of the GDPR

1. Breach of the obligation to have legal basis for the processing carried out

Article 6 of the General Data Protection Regulation provides 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."

To be lawful, the processing of personal data must therefore be based on one of the legal basis referred to above.

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

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.

This processing is carried out by the company for commercial purposes only.

As part of the investigations carried out by 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.

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

Furthermore, given the nature of the processing in question, the legal basis 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.

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 as a preliminary point 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.

By way of illustration, the Article 29 working party (called "G29" now the European Data Protection Board (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 "*publicly available data are still personal data subject to data protection requirements*". While acknowledging the fact that personal data are 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).*"

Furthermore, in order for the data controller to be able to avail itself of these legal basis, 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.

In the present case, even if the interests of the company 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 data subjects 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 opinion of the EDPB on the aforementioned notion of legitimate interest.

In the present case, the processing presents a particularly strong intrusiveness: it collects from a given individual a large number of photographic data, which are associated with other personal data likely to reveal various aspects of their private life. Based on that data, a biometric template, i.e., biometric data that can, if reliable, be used to uniquely identify the individual from a photograph of the individual: the holding of such data by a third party constitutes a significant invasion of privacy. Finally, it should be noted that this processing concerns an extremely high number of individuals.

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 the personal data would be processed by Clearview. 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.

It must therefore be considered that individuals who have published photographs 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 a facial recognition program (which combines the image of a person 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.

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

Consequently, the company has no legal basis for the processing in question, in breach of Article 6 of the Regulation.

2. A breach of the obligation to respect the right of access

Article 15 GDPR provides: "*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.

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

In the present case, it stands out from Referral No. 20012263 that the complainant asked the company for access to the data concerning her 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 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, after further exchanges relating to the transmission of an ID and in the absence of a satisfactory response, the appointed third party sent an order to the company.

The company provided a response to the access request which, first of all, is 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.

Secondly, 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 did not facilitate the exercise of the complainant's rights.

Finally, it stands out 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.

It stands out from these elements that the company does not effectively respond to requests for access made to it under Article 15 of the GDPR and does not facilitate the exercise of the right of access of data subjects.

All of these facts constitute a breach of Articles 12 and 15 of the Regulation.

3. A breach of the obligation to respect the right to erasure

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*."

It stands out from Referral No. 20012263 that the complainant received no response from the company concerning the erasure of her data she required

However, since the Commission considers that the processing carried out cannot be based on any valid legal basis in the light of European regulations, erasure was legally binding.

This element constitutes a breach of Article 17 GDPR.

Consequently, CLEARVIEW AI, located at 214 W 29TH ST NEW YORK CITY, NY 10001 – United States of America, is hereby formal notified, within two (2) months of notification of this Decision, and subject to any measures it may have already adopted, to:

- **not carry out the collection and processing of personal data relating to data subjects who are on French territory, without legal basis, as part of the operation of the facial recognition software which it markets, and in particular, delete all the personal data of such individuals (after responding to the access requests already made where applicable);**
- **facilitate the exercise of data subject rights and in particular, effectively respond to the complainant's request for access;**
- **honour the request for erasure made by the complainant in question;**
- **provide supporting documentation to CNIL that all of the aforementioned claims have been complied with within the time limit set.**

At the end of that period, if CLEARVIEW AI has complied with this order, it will be considered that these proceedings are closed and a letter will be sent to it to that effect.

Conversely, if CLEARVIEW AI has not complied with this order by the end of that period, a rapporteur may be appointed who may request the restricted committee to issue one of the sanctions provided for by Article 20 of the amended French Data Protection Act of 6 January 1978.

The Chair

Marie-Laure DENIS