SEE ALSO Press release of 9 March 2022

[doc. web n. 9751362]

Injunction Order Against Clearview AI - February 10, 2022

Record of measures

n. 50 of 10 February 2022

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stanzione, president, Prof. Ginevra Cerrina Feroni, vice president, Avv. Guido Scorza, member and the cons. Fabio Mattei, general secretary;

GIVEN the Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, concerning the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data and which repeals Directive 95/46 / EC (General Data Protection Regulation, hereinafter the "Regulation");

GIVEN the Code regarding the protection of personal data (Legislative Decree 30 June 2003, n.196), as amended by Legislative Decree 10 August 2018, n. 101, containing provisions for the adaptation of national law to the aforementioned Regulation (hereinafter the "Code");

GIVEN the Regulation n. 1/2019 concerning internal procedures with external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor for the protection of personal data, approved by resolution no. 98 of 4 April 2019, published in the Official Gazette n. 106 of 8 May 2019 and in www.gpdp.it, doc. web n. 9107633 (hereinafter "Regulation of the Guarantor no. 1/2019");

GIVEN the documentation in the deeds;

HAVING REGARD to the observations made by the Secretary General pursuant to art. 15 of the regulation of the Guarantor n. 1/2000;

SPEAKER Attorney Guido Scorza;

WHEREAS

1. INTRODUCTION

The proceeding originates from a complex preliminary investigation launched ex officio following press reports that revealed the existence of various problems relating to the facial recognition products of the US company Clearview AI Inc. (hereinafter

"Clearview" or "Company").

Over the course of 2021, the Office received four complaints filed against Clearview. In particular:

- on February 24, 2021 by Mr. XX (issue no. XX);

- on March 22, 2021 by Mr. XX (issue no. XX);

- on 1 June 2021 by Mr. XX (issue no. XX);

- on July 22, 2021 by Mr. XX, who complained about the lack of response to requests for access to data pursuant to art. 15 of the GDPR, also following two reminders on 25 May and 18 June 2021 (file no. XX).

Complainants XX, XX and XX reported the fact that the processing of their data took place without consent and reported on Clearview's request to send a copy of a personal identity document to follow up on the access requests presented.

From the documentation attached to the complaints, the Office found that Clearview responded to the access requests of complainants XX, XX and XX through specific reports containing the results of the search generated by the software. In particular, it emerged that:

- with reference to Mr. XX, the Company has in its database three images indexed through the following URLs:

https: // ...;

https: // ...;

https: // ...

- with reference to Mr. XX, the Company has in its database 13 images indexed through the following URLs:

https: // ...

https: // ...

https: // ...

https: // ...

http: // ...

https: // ...

https: // ...

https: // ...

https: // ...

https: // ...

https: // ...

https: // ...

https: // ...

- with reference to Mr. XX, the Company has in its database 9 images indexed through the following URLs:

http: // ...

https: // ...

https: // ...

https: // ...

https: // ...

https: // ...

https: // ...

https: // ...

http: // ...

The Authority also received two reports from two organizations committed to the defense of privacy and the fundamental rights of individuals.

With a note dated February 19, 2021, the XX association, in addition to reporting the precedents of the Swedish and German authorities, brought to the attention of the Authority significant critical issues regarding the legal basis of the treatment put in place by Clearview, as well as in relation to the procedures adopted. by the company regarding the right of access (file no. XX).

On 7 September 2021, the same association sent a further report in which it asked the Office to ascertain the use of the services offered by Clearview by the State Police.

On May 25, 2021, organization XX reported critical issues to the Office regarding the processing carried out by Clearview, in particular with reference to the legal basis, compliance with the general principles on data protection and the risks to rights and freedoms data subjects' use of the Clearview product by law enforcement authorities (File No. XX).

2. INSTRUCTORY ACTIVITIES

With a note dated 25 March 2021 (prot. Of the Guarantor no. 16155/2021), in response to the Authority's request for information of 9 March 2021, the Company argued that the Regulation is not applicable and therefore the lack of jurisdiction of the Guarantor Italian. In particular, he stated i) not to offer products and services in Italy as it has adopted technical measures aimed at blocking any attempt to access the platform by Italian IP addresses and ii) not to carry out any monitoring pursuant to art. 3, par. 2, lett. b) of the Regulations as the concept of monitoring implies continuous and ongoing observation where the only product of Clearview AI is an application for searching images that provides search results with links to third-party websites. This technology, therefore, according to the Company, would not track or monitor people over time, but would resolve itself in a snapshot of the search results at the time of the search, comparable to the search operations carried out by Google Search. The Company reported that it does not hold any list of Italian customers, that it has not included any reference to the Regulations in the privacy policy and that it has not appointed a representative pursuant to art. 27, as this rule, like the rest of the Regulation, would not be applied to the activity it carries out.

With a note dated 22 April 2021 (prot. No. 22235/2021), the Office, on the basis of the elements acquired, notified Clearview, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the measures referred to in art. 58, par. 2, of the Regulations, concerning the alleged violations referred to in Articles 5, par. 1 letter a), b and e), 6, 9, 12, 13, 14 and 15 and 22 of the Regulations.

With the same note, the Company was invited to produce defensive writings or documents to the Guarantor or to ask to be heard by the Authority (Article 166, paragraphs 6 and 7, of the Code).

With a note dated 22 June (prot. 30787/2021), Clearview filed its defense, stating that:

- since the end of 2019, the US law enforcement agencies have promoted the use of Clearview products, especially in the context of investigations into child pornography. This sparked international interest in Clearview products which led to trial accounts being signed by European government agencies for a short period of time;
- in March 2020, following the complaints received through the European supervisory authorities, these test accounts, however small in number, were all closed and deactivated;
- Clearview currently no longer has any European test users, nor customers established in the European Union: this is ensured by a precise setting that prevents access to the software via European IP addresses;
- the technology underlying the service is aimed at improving public safety, reducing investigation times and assisting law

enforcement in identifying criminals (including violent criminals, pedophiles and drug traffickers). The Company highlights how these activities are carried out and under the direct control of the public authorities who, under their responsibility, decide to use the Clearview software; the use of the software is subject to the conditions of use, which provide that it is the customer's responsibility to verify that the use of this product is legitimate in light of the local regulations applicable to it. Therefore, as with any technology supplier, it is not the Company's responsibility to deal with the use of the technology or devices by customers;

- the assessment of the legal basis for the use of the software by customers or potential customers cannot be a mission or responsibility of Clearview;

- the Company contractually requires its customers to conduct further investigations in order to independently corroborate all information collected using Clearview technology, primarily the identification of the subject through its software; no decision, to the best of the Company's knowledge, is made solely on the basis of the data provided by the Clearview software;

- with regard to jurisdiction, the Company, after having remembered that it is based in the U.S.A. and not to have any branch in the European Union, argues the inapplicability of art. 3, par. 1, of the Regulation as it is not established in the Union or in Italy and the inapplicability of art. 3, par. 2, of the Regulation (targeting criterion) both in terms of the offer of goods and services to interested parties who are in the Union and the monitoring of their behavior to the extent that the monitoring takes place in the Union;

- with reference to the criterion of the offer of goods and services, regardless of the obligation of a payment by the interested party (Article 3, paragraph 2, letter a) of the Regulation), the Company reiterates that it does not offer goods and not to provide services to European customers. The Company maintains, on the basis of the provisions of the Personal Data Protection Committee in guidelines no. 3/2018 and by Recital 23 of the Regulation, that the analysis of the existence of the criterion in question must be carried out in the sense of ascertaining whether Clearview's sales activity is intentionally, and not inadvertently or accidentally, aimed at subjects who are in the Union.

The Company believes that the arguments put forward by the Guarantor in the dispute pursuant to art. 166 of the Code are not suitable to prove the existence of the criterion for the following reasons:

- it is true that, in the past, Clearview has offered its products in Canada as it is a market in which, for reasons of proximity to the US market, expansion is quite natural; however, following the proceedings initiated by the Canadian Privacy Commissioners, the Company has ceased all processing activities in that country and this cannot be an element that

demonstrates its intention to enter the Italian market;

- the journalistic sources according to which Clearview intends to expand its activities in several countries including, in particular, Italy, are not usable: these are speculations based on the fact that the Company previously had trial users in the Union European Union and cannot be used to deduce its intention to offer products or services in Italy;

- Clearview has received unsolicited requests for access to trial accounts from European users, but those accesses are no longer available as the Company has decided to no longer offer its product in the context of the European Union, before that that the Guarantor initiated the present investigation; moreover, the concept of "intention" (to provide services to data subjects in one or more EU Member States) mentioned in Recital 23, must be interpreted, in accordance with guidelines 3/2018, as a deliberate and existing and not hypothetical intention and future;

- the measure adopted by the Swedish Data Protection Authority concerns one of the test accounts mentioned above and now no longer available. Furthermore, these accounts were never made available to individuals and in fact, in the Swedish decision, it appears that the software was used by the Swedish law enforcement agencies;

- with reference to the criterion for monitoring the behavior of data subjects who are in the European Union, to the extent that such behavior takes place within the Union (Article 3, paragraph 2, letter b), of the Regulation) , the Company observes that, from Recital 24, the criterion in question refers to processing activities that allow monitoring of the behavior of the data subjects, including the potential subsequent use of personal data processing techniques. These techniques consist in profiling a natural person, in particular, in order to make decisions concerning him or to analyze or predict his preferences, behavior and personal attitudes; from this definition, it emerges that not any monitoring is relevant, but only those that concern or refer to the behavior of the interested parties, to be understood as specific actions they put in place (for example, what they buy, where they go, how they live);

- in light of the aforementioned definition of monitoring, Clearview believes that it does not carry out processing activities aimed at analyzing the behavior of the data subjects, nor does it create any "profile" attributable (related to) to a natural person: Recital 24 of the Regulation states that a processing activity can potentially be considered a monitoring, if "natural persons are tracked on the Internet, including any subsequent use of personal data processing techniques that consist of profiling a natural person". The term “tracking” is not defined, but the meaning of the verb must be understood in the sense that a person is followed in time. The term "profiling" (profiling) is defined in art. 4, par. 1, no. 4, of the Regulations and indicates "any form of

automated processing of personal data consisting in the use of personal data to evaluate certain personal aspects relating to a natural person". Furthermore, the Committee explains that the term "monitoring" implies that the data controller has a specific purpose for the collection and subsequent reuse of data concerning the behavior of an individual within the Union;

- Clearview's sole purpose is to offer a search engine to allow its customers to search for images on the Internet. The facial vectors that the Company uses to search for images cannot be used to infer or mathematically derive information about a person, because they are not linked to the name and / or position and / or other identifiers. Even if a facial vector is obtained, it could not be analyzed to reveal intelligible information about a person's facial features. Tracking over time is not possible because a search always produces only the results available at the time of the search. Therefore, even a comparison between searches carried out at different times does not allow to trace a person; what can happen is that a police officer finds an investigative clue and then conducts specific investigations which, however, are not carried out by the Clearview software. Certainly, the Company concludes, this is not a tracking by automated means. The same applies to profiling as, according to the Company's reconstruction, a police officer can draw conclusions about a person, for example because the search for images produces a match with the suspect, but these conclusions are not drawn based on the software. by Clearview, as the information comes from third-party sites;

- to be considered a monitoring according to the criterion in question, the data processing carried out by the data controller must be aimed at carrying out any subsequent behavioral analysis or using profiling techniques. Clearview does not pursue nor would it potentially be able to achieve these objectives from a technical point of view;

- the Guarantor itself does not seem able to indicate unequivocally whether the activity carried out by Clearview constitutes a monitoring (behavioral monitoring only) or a profiling activity despite, as already represented, profiles of the interested parties are not created, nor is it performed an analysis of their behavior;

- Clearview asserts that the mere collection of data, even of a significant volume, does not automatically constitute a monitoring;

- the Article 29 Working Group on automated decision-making relating to natural persons and profiling (Guidelines WP251), on page 7, states that the use of the verb "evaluate" suggests that "profiling involves some form of evaluation or judgment about a person. The simple classification of people based on known characteristics such as age, gender and height does not necessarily lead to profiling. The latter in fact depends on the purpose of the classification ". The example provided in the

guidelines on the same page clarifies the point even better where it states that "a company may wish to classify its customers based on age or gender for statistical purposes and to acquire an aggregate overview of their customers without carrying out forecasts or draw conclusions about a specific person. In this case, the purpose is not the evaluation of individual characteristics and therefore it is not a question of profiling ". From this it is clear that the purpose is the decisive element in assessing whether the processing falls within the definition of profiling;

- the WP251 guidelines, on the same page, referring to the recommendation CM / Rec. (2010) 13 of the Council of Europe, specify that the profiling activity is divided into three phases: i) data collection; ii) automated analysis to identify correlations; iii) application of the correlation to a natural person to identify present or future behavioral characteristics. The indication is added that "the data controller who carries out the profiling must ensure that he meets the requirements of the regulation in relation to all the above steps". Even assuming the Clearview system is involved in the first two phases, it is clear from the facts that the third phase is peacefully outside of what the Clearview software can do and the Company's business position. If present or future behavioral characteristics of a natural person are identified through the use of the search results provided by the software, the data controller is not Clearview, but the customer who purchases the service. The Swedish authority stressed in its decision that the Swedish police (and only the police), as a customer of the software, were the data controller and that they were independent of Clearview, the provider of the search tool;

- Clearview collects images and tags relating to the Internet sources from which they are collected. Only when a customer queries the database, submitting an image to be searched for, is it compared with those collected by Cleraview. Once the correspondence between the images has been verified, the customer receives the result and Clearview achieves its commercial purpose by offering the correspondence between images previously subjected to a hashing process; all subsequent activities and the related data processing carried out by the customer do not fall within the scope of Clearview's activity but relate to a distinct commercial decision based on the purposes pursued by the customer as an independent data controller;

- moreover, art. 3, par. 2, lett. b) does not apply generically to profiling, but refers to the monitoring of behavior and therefore requires that the data controller's processing activities are carried out to obtain an analysis of the behavioral habits of individuals, purposes that Clearview clearly does not pursue and does not achieve. . The Company does not classify individuals in any way. Furthermore, the software is unable to evaluate, judge, or predict behavior; the data provided to the

customer is simply made up of images, metadata (if any) and their source (URL) on the Internet at the time of the search;

- with regard to the geolocation data referred to in the Clearview privacy policy, the term geolocation means only the location metadata embedded in the photo, which indicate where the same was taken. Clearview does not provide such location metadata to customers, but if an online photo has embedded location metadata, the customer can see it of the photo when using the URL link of the photo, just like anyone else viewing the photo on the Internet;

- finally, with reference to the request of the complainant XX to provide a copy of his identity document, disputed as deemed unjustified, the Company requires persons, who make a request for access to data, to provide an official identification photo. Clearview has no means of verifying the identity of the persons appearing in the images it collects and does not retain any information about people's names, email addresses, residency or identity, as also clearly emerges from the facial search results. (Face Search Results) that Clearview provides in response to data access requests. From the simple indication of the name it is impossible for the Company to know if the person who makes a request for access to the data is present in the database; to activate the search, therefore, the Clearview software needs a photo for the relative confirmation and, in order to avoid fraudulent requests, the Company has decided that this photo must be the one present on an official document, such as an identity card . The Company does not keep the images of the identity card, nor use them for other purposes. This request does not seem excessive given that art. 12, par. 6, of the Regulation expressly provides that "[...] if the data controller has reasonable doubts about the identity of the natural person who submits the request referred to in articles 15 to 21, he may request the provision of further information necessary to confirm the identity of the interested party ";

- with reference to complaints XX and XX, the Company reiterates that it is not subject to the Regulation and that the privacy policy is consequently compliant with US standards. However, the Company is willing to act spontaneously to resolve the complaints of the complainants and therefore to delete all images and links produced by the image search for the photos provided by the two complainants. The Company has spontaneously extended the rights of the data subjects to European residents as a gesture of goodwill and transparency and it is with the same spirit that it offers the deletion of images and links relating to the complainants, however this cannot be understood as acceptance of the Italian jurisdiction and / or applicability of the GDPR, which are contested and strongly denied.

With a note dated 12 October 2021 (prot. No. 50926/2021), the Office, following the receipt of complaints XX and XX, notified Clearview, pursuant to art. 166, paragraph 5, of the Code, a supplementary dispute with the simultaneous initiation of the

procedure for the adoption of the measures referred to in art. 58, par. 2, of the Regulations, concerning the alleged violations referred to in Articles 5, par. 1 letter a) and b), 6, 9, 12, 13, 15 and 27 of the Regulation.

With the same note, the Company was again made aware of the possibility of producing defensive writings or documents and possibly asking to be heard by the Authority (Article 166, paragraphs 6 and 7, of the Code).

With a note dated 11 November 2021 (prot. No. 56766/2021), Clearview presented its defense statement, declaring that:

- the Company does not operate in any member state of the European Union, does not monitor the behavior of interested parties who are in it and therefore no European Authority has jurisdiction over its activity, unless it violates the international principle of territoriality;

- there is no legal basis that justifies administrative proceedings against companies not established in Italy and which do not do business in Italy; a proceeding of this kind would violate the public order of the U.S.A .;

- with specific reference to the Regulations, the Company reiterates the non-applicability of art. 3, par. 2, lett. a) and b), which establishes the criteria for applying the Regulation to companies not established in the European Union;

- in particular, art. 3, par. 2, lett. a) of the Regulation would not be applicable because Clearview does not offer products and services in the Union, as already pointed out in the previous correspondence. The Company reiterates that it provides an image search engine for law enforcement agencies outside the Union;

- moreover, art. 3, par. 2, lett. b) applies to "monitoring the behavior" of data subjects in the Union. Although there is no definition of monitoring, the word itself and the rationale of art. 3 clarify that the observation of a natural person is required for a certain period of time;

- Recital 24 specifies that in order to determine whether a treatment consists of monitoring a behavior, it must be verified whether the natural person is tracked on the Internet. In this regard, the contribution of Thaomas Zerdick, a member of the drafting team of the European Commission on the Regulation, is cited, who argues that the tracking underlying art. 3, par. 2, lett. b) it must be equivalent to the surveillance of a person (citing as an example systems that take photographic snapshots compared to real-time monitoring systems);

- Clearview's search engine only provides snapshots of photos available on the Internet at the time the customer searches. The Company does not collect or provide any information on the location, browser history, commercial activity or behavior of the natural person that appears as a result of the search and does not imply any behavioral, predictive or analytical model. The

information that can be obtained about a person using the Clearview search engine is less significant than what can be obtained from a Google Search search based on that person's name and no one claims that a browser search of Google constitutes behavioral monitoring;

- if, for example, a search were made on Google Search with the names of the complainants, limiting it to images, the answer would provide the photos, probably of the complainants, as they are freely available on the Internet. Furthermore, by clicking on the results, the URL would direct you to the websites where the photos appear and from which further information could be obtained (the Company provides screenshots of a similar search carried out on Google search with the names of the complainants XX and XX);

- as is known, the Google search engine does not monitor people as it is, rather, an algorithm that makes the information published on the Internet accessible. Google provides a snapshot of the most relevant pieces on a specific search at the time of the search. The same happens with the results obtained following a research done with the Clearview product. There may be leads for further research, but nothing more;

- from the text of Recital 24 of the Regulation it clearly emerges that the legislator intended to refer to a subsequent use of the information deriving from the tracking of the person for whom constant monitoring is the prerequisite for any "subsequent use"; Clearview's technology does not produce such information, but only the results of a search that the customer can then use to make further ones, also on the basis of other sources of information. Clearview is just a search engine;

- the Company only provides a tool, it is not the owner of the research conducted by the user of the tool and of any subsequent use of the results of the research. It is the Clearview customer who decides to use the search engine to search for their images, uploading an image to obtain the corresponding results. It is the customer who decides what to do with the search results. Therefore, it is the customer who decides whether the tool can be used within a specific regulatory framework and Clearview is paid for the tool, not for the search results or for what the customer will do with the search results;

- this interpretation is confirmed by art. 25, par. 1, of the Regulation, which establishes that the owner, when determining the means of processing, must ensure that the parameters of the Regulation are respected. Consequently, it is the responsibility of the customer, who is the data controller, to determine whether and how to use the Clearview search engine. This approach also explains why the Swedish and Finnish personal data protection authorities have initiated proceedings against national law enforcement agencies and not against Clearview;

- the Guarantor must also take into account the fact that the Company has implemented technical measures to ensure that searches cannot be carried out from the European Union or from Italy. These measures were adopted in order to remove any doubts under European law, given that the product is not offered to or within the European market;

- the Company therefore requests that the Guarantor close the proceeding due to lack of jurisdiction;

- in a globalized world it is impossible to take all existing laws into consideration when designing a product; Clearview complies with US law and, as the Regulation does not apply to its services, there is no need to examine it further. Moreover, given that it is assumed that the Google search engine complies with European laws as Google is established in the Union and offers its services to users in the Union, even if the Regulation is deemed applicable to Clearview, the processing of data of the complainant should be considered lawful;

- although the Company does not offer its products in the European Union and the Regulation does not apply, Clearview spontaneously complies with the access requests of European residents;

- the Company fulfilled the request of the complainant XX on April 29, 2021 and responded to the request of the complainant XX on September 29, 2021, before the notification of the supplementary contestation by the Guarantor;

- The Company takes the complaints of complainants seriously and offers to implement measures to ensure that the two persons concerned are no longer searched on the Clearview search engine. Since these are measures that involve costs and resources, the Company asks if the intervention could help define the cases.

3. RESULTS OF THE INVESTIGATION ACTIVITY

3.1 CHARACTERISTICS OF THE OFFERED SERVICE

Clearview is a company, headquartered in the United States, established in 2017 that created a facial recognition search engine. On the basis of the information that emerged during the mutual assistance with other European supervisory authorities, from the information disclosed by the Company itself and from the complaints and reports received by the Guarantor, it appears that the facial recognition platform developed by Clearview allows the search for images internal database. The Company, in fact, collects, through web scraping techniques, images from social networks (e.g. Twitter or Facebook), blogs and, in general, from websites containing publicly accessible photos, but also from videos available online (e.g. . on Youtube). The images thus collected are processed with biometric techniques in order to extract the identifying characteristics of each of them and, subsequently, transformed into "vector representations". These representations, made up

of 512 vectors that trace the different unique lines of a face, are subsequently hashed for the purpose of indexing the database and subsequent research. The Company therefore creates biometric templates which, in the research phase, are subjected to comparison with the sample being researched, generating a 1 to N (one to many) verification process. The image hash, the unique identifier of each image (a sort of facial fingerprint), facilitates, as mentioned, indexing and subsequent research. The platform was clearly created in order to generate high quality investigation leads.

Each image can be enriched with associated metadata (for example, the title of the image or web page, the link of the source, the geolocation, the gender, the date of birth, the nationality, the language) so that when the software identifies a correspondence, extracts all the related images from the database and presents them to the customer of the service as a result of the search together with the associated metadata and links, thus allowing to go back to each single source page.

An image collected in this way remains in the database even in the event that the original photo or the reference web page is subsequently removed or made private.

As evidenced by the company's website (https: // ...) the platform "includes a database of over 10 billion facial images extracted from public web sources, including news media, mugshot websites, public social media and other sources of public access ".

The machine learning technology underlying the Clearview platform was the subject of a patent application filed in February 2021 with the US Patent & Trademark Office on February 11, 2021 and with the World Intellectual Property Organization.

This request shows that the technology, called "Method for providing information about a person based on facial recognition", includes various methods for providing information about a person based on facial recognition and various applications of the same, including face-based check -in, face-based personal identification, face-based identity verification, face-based background checks, facial data collaborative network, related face search, and face-based personal identification. These methods are represented as capable of providing accurate information about a person in real time.

The patent application submitted by the Company itself offers precise details on the operation of the technology. The system runs through the following steps: i) reception of facial image data that includes at least one facial image of the subject from a user's device; ii) transformation of facial image data into facial recognition data; iii) comparison, via server, of the reference facial recognition data with the facial recognition data associated with a plurality of stored facial images in order to identify at least one probable candidate corresponding to the captured image; iv) on the basis of the identification of the candidate

corresponding to the acquired facial image, retrieval from the database of the personal information associated with the candidate; v) return of personal information to the user's device with assurance that this device displays personal information.

Clearview, therefore, not only collects images to make them accessible to its customers, but processes the images collected by web scraping, through a proprietary facial matching algorithm, in order to provide a highly qualified biometric search service.

Furthermore, according to the information available on the Clearview website, the free service offered is not freely accessible to the public, but is intended for certain categories of customers (i.e. police forces).

The profiles just described lead us to believe that the platform offered by Clearview takes on peculiar characteristics that differentiate it from a common search engine that does not process or enrich the images on the net. In particular, Clearview does not work on cache memory, but creates a database of snapshots of images that are stored as present at the time of collection and not updated. Furthermore, as mentioned, Clearview processes these images with biometric techniques, hashes them and associates them with any available metadata.

The statements made by the Company according to which the service it offers is comparable to that offered by Google Search therefore appear to be completely groundless.

3.2. EXISTENCE OF THE EUROUNITY JURISDICTION

Art. 3 of the European Regulation n. 2016/679 governs its own "Territorial scope" by identifying different conditions depending on whether or not the data controller is established in the territory of the European Union.

In the case in question, Clearview has not identified an establishment in Europe and therefore, in order to conduct an assessment regarding the applicability of the European legislation on the protection of personal data to the processing carried out by the Company, it is necessary to verify the existence of criteria pursuant to art. 3, par. 2, of the Regulation (so-called targeting). These criteria are identified in the offer of goods or services to interested parties who are in the Union or in the performance, with respect to the latter, of an activity related to the monitoring of their behavior, to the extent that the latter takes place in the 'Union.

Preliminarily it must be said that, for the purposes of applying the targeting criterion, the data being processed must relate to data subjects in the Union. In the present case, the fact that Clearview processes personal data of subjects located in the European Union and, in particular in Italy, is clear from the feedback that the Company has provided to the complainants, from which it appears peacefully that they have been collected images of the same, that these images have been associated with

metadata and subjected to biometric processing (these images are, in fact, the result of the identification resulting from the comparison of the data stored in the database with the sample provided by the complainants), but also, indirectly, from the evidence that emerged in the context of the proceedings initiated by the European supervisory authorities (see decision of the German supervisory authority of the Land of Hamburg (decision 545/2020; 32.02-102) and of the Commission Nationale de l'Informatique et des Liberté (CNIL, Decision n ° MED 2021-134 of 1st November 2021 issuing an order to comply to the company CLEARVIEW AI).

ART. 3, PAR. 2, LETT. A), OF THE REGULATION

As for the first of the profiles considered (see Article 3, paragraph 2, letter a) of the Regulation), Clearview, during the procedure, declared that it does not offer services in Europe and that it does not have European customers using the system. facial recognition device produced by the Company.

The considerations made by the data controller are however denied, with reference to what has happened so far, by the provision recently adopted by the Swedish supervisory authority (DI-2020-2719: A126.614 / 2020 of 10 February 2021) regarding the occurrence use of the facial recognition system offered by Clearview by subjects belonging to national law enforcement agencies, the latter circumstance which presupposes, from origin, the use of the relative service by European users.

Furthermore, as stated by Clearview with the aforementioned note of 22 June (prot. , inhibiting access to European IPs. Therefore, by Clearview's own admission, up to a certain date the Company directed - and had the intention to do so - its services also in Europe.

For the purposes of the applicability of the targeting criterion referred to in art. 3, par. 2, lett. a) of the Regulation, on the basis of the indications contained in the "Guidelines 3/2018 on territorial scope", adopted by the Committee for the protection of personal data on 12 November 2019, it is required that the conduct of the "data controller, who determines the means and purposes of the processing itself, demonstrates [i] its intention to offer goods or services to an interested party who is in the Union "(see par. 2.a of the aforementioned Guidelines). In particular, Recital 23 of the Regulation establishes that "[m] between the simple accessibility of the website of the data controller, the data controller or an intermediary in the Union, an e-mail address or other contact details or the use of a language usually used in the third country in which the data controller is established are insufficient to ascertain this intention, factors such as the use of a language or currency usually used in one or

more Member States, with the possibility to order goods and services in that other language, or the mention of customers or users located in the Union may highlight the intention of the controller or processor to offer goods or services to data subjects in the Union '.

The Court of Justice of the European Union itself (Pammer / Reederei Karl Schlüter GmbH & Co and Hotel Alpenhof / Heller (joined cases C-585/08 and C-144/09) has indicated some factors in the presence of which it can be considered that a commercial activity carried out by a subject is directed towards a Member State, citing, among others, the fact that the European Union is mentioned in reference to the good or service offered, the international nature of the activity or the start advertising and marketing campaigns targeting the public of an EU country.

The intention of the data controller to address the European market, as well as confirmed by the decision adopted by the Swedish Data Protection Authority mentioned above and by the aforementioned note of June 2021, also clearly emerges from the terms in which the privacy was formulated. policy prior to the changes made starting from 20 March 2021, or in a time that can be placed between the first request for information by the Guarantor, dated 9 March 2021, and the subsequent feedback provided by the company on 25 March 2021.

Until then, said information contained, in fact, a series of indicators from which it was possible to infer the will of the data controller to address the offer of its service also to users of the European Union, including the legal basis of the processing, online. with the provisions of art. 6 of the Regulation, the commitment to adopt adequate guarantees to comply with the rules on the protection of personal data any transfer of data outside the European Economic Area and the provision of the possibility for residents of the European Economic Area or Switzerland to lodge a complaint with the competent data protection authority regarding the processing carried out against them by Clearview.

In particular, two points of the information seem relevant, the one on "Independent Recourse" and the next on "International Transfers". The first reads that "Residents of the European Economic Area or of Switzerland who wish to submit a complaint or seek resolution of a dispute related to Clearview AI's processing of personal data may seek appropriate recourse free of charge by contacting the appropriate Data Protection Authority (DPA) in their respective country "[emphasis added], while in the second it is specified that" The personally identifiable information we receive in the computers and systems of our offices in the United States is processed by us in the United States, where laws regarding data protection may be less stringent than the laws in your country. When personal data is transferred outside the EEA, we will put in place suitable safeguards to ensure

that such transfer is carried out in compliance with applicable data protection rules. Clearview deeply values user privacy and data security controls; our cybersecurity infrastructure includes technical and policy controls that are consistent with the requirements of General Data Protection Regulation ”[emphasis added].

In addition, with specific regard to the recipients of the service, the "Terms of use of the service", applicable starting from 17 January 2020, provided that "User" was to be understood as "each organization (...) and all persons who access the Service as a User executive or Users allowed ", thus describing suitable categories to encompass a wider audience than that constituted only by the law enforcement agencies to which Clearview has instead referred in its reports, confirming, moreover, that it has made a series of accounts available to European government agencies trial until March 2020.

Art. 3, par. 2, lett. b) of the Regulation

The second of the targeting criteria identified, or the one referred to in art. 3, par. 2, lett. b), traces the application of the European Data Protection Regulation to the processing activities related to the monitoring of the behavior of data subjects in the European Union that takes place within the Union.

The nature of the processing activity that can be considered behavior monitoring is specified in Recital 24 of the Regulation, which provides that in order to "establish whether a processing activity is similar to monitoring the behavior of the data subject, it is appropriate to check whether the natural persons are tracked on the internet, including any subsequent use of personal data processing techniques that consist in profiling the natural person, in particular to make decisions concerning him or her or analyze or predict his preferences, behavior and personal positions " .

The Guidelines 3/2018 mentioned above specify that, for the purposes of the operation of the provision, it is not necessary to investigate the existence, in the head of the data controller, of the intention to "address a subject", but that, however, " the use of the word "monitoring" implies that the controller has a specific purpose in mind for the collection and subsequent re-use of relevant data on the behavior of a natural person within the EU "(see par. 2. c of the aforementioned Guidelines) and that, in this regard, it is essential to assess whether there is a tracking of natural persons on the Internet, including any subsequent use of profiling techniques.

The processing carried out by Clearview consists, as represented, in the collection of images from the web (so-called web scraping) and in their processing with automated tools in order to create vector representations of faces and, subsequently, subject them to hash to index the data. , an operation necessary to establish a possible correlation with the images being

compared uploaded by users. The activity carried out therefore does not appear to be superimposable, as instead declared by the company, to that carried out by any search engine, taking into account the fact that the owner performs a technical reworking of the images collected, so as to make them "biometric data", to which, moreover, information certainly suitable for identifying the person portrayed are associated.

The information published on the Clearview website indicates, in fact, among the collected data, in addition to the photographs accessible to the public and available on the Internet, also the information that can be extracted from these photographs, such as the geolocation metadata that the latter may contain, as well as those derived from the analysis of the faces of the people depicted and which, as such, constitute, as mentioned, biometric data on the basis of which the comparison process is performed.

But it is precisely this last step that constitutes the key to reading the entire collection and processing process put in place by Clearview which aims to constitute a data set to which the images uploaded by the user can be compared and then extracted from the its archive, the images that can be associated with them from a biometric point of view, as well as related information.

The search mechanism therefore proves to be a means of activating a comparison process that qualifies the purpose of the processing carried out by the supplier company, as well as that carried out by the customers who use the service. There is therefore a correlation between the two types of processing which, moreover, is also recognized within the European Regulation when, for the purpose of applying the targeting criterion, it recalls the circumstances in which "the processing activities are related to (...) b) the monitoring of their behavior as far as their behavior takes place within the Union ".

The information in question is archived in the Clearview database and is enriched over time with others extracted from new templates suitable to also reflect the physical changes that the same subject has had, as emerges from the examination of some of the complaints proposed to the Authority (cf. . in particular the one presented by Mr. XX). It follows that Clearview does not offer a simple match as a search result, but also a repository of resources that winds through time. The assessment of this circumstance, together with the comparative purpose highlighted above, is suitable for integrating, as required in Recital 24, an activity similar to the control of the behavior of the interested party as it is carried out through internet tracking and subsequent profiling.

Unlike what Clearview argued in its defense (see note no.33759 of 22/06/2021), the activity carried out by the same does not seem to be attributable to a mere classification of individuals on the basis of known characteristics such as age, gender and

height, as a further activity is carried out consisting in the extraction of biometric data from the images collected on the web, using them for comparative purposes and then also retrieving the information associated with them. The same Company, in the patent application filed with the US Patent & Trademark Office on 11 February 2021, in describing the purposes of the processing carried out through the use of facial recognition tools, highlights the potential aptitude of a system of this type to be used for the purpose of acquiring accurate information about people and evaluating specific characteristics. And it must be considered that even the search engines, to which Clearview tries to assimilate its business, put in place a type of treatment which, even if carried out with tools other than those used by the Company, can have the effect of building a personal profile of the interested party - to whom the research refers - by virtue of the association created among the information resulting from it. In this regard, it should be considered that the Court of Justice of the European Union, with the ruling of 13 May 2014 case C / 131-12 (so-called Google Spain), found that the operator of a search engine distinct from that carried out by the publishers of the websites, to which it is added, as it allows the data to be made accessible "to any Internet user who performs a search starting from the name of the person concerned, even to those users who would not otherwise have found the web page on which these same data are published "(see paragraph 36 of the judgment), also specifying that" the organization and aggregation of information published on the Internet, created by search engines in order to facilitate their users 'access to said information, may have the effect that such users, when their search is carried out starting from the name of a natural person, obtain through the list of results a visio overall structured information relating to this person available on the Internet, which allows them to establish a more or less detailed profile of the latter "(see point 37 of the same).

Art. 4, par. 1, no. 4, of the Regulation describes "profiling" as "any form of automated processing of personal data consisting in the use of (...) personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning the performance professional, economic situation, health, personal preferences, interests, reliability, behavior, location or travel of that natural person ".

Based on the provisions of the "Guidelines on the automated decision-making process relating to natural persons and on profiling", adopted by the Personal Data Protection Committee on 3 October 2017 and amended on 6 February 2018, "the widespread availability of personal data on Internet and those obtainable from Internet of Things devices, associated with the ability to find correlations and create connections, can allow the determination, analysis and prediction of aspects of a person's personality, behavior, interests and habits " . The aforementioned guidelines identify three specific phases that characterize the

profiling activity, establishing that it must a) concern personal data, b) be a form of automated processing and c) be aimed at evaluating personal aspects relating to a natural person.

These phases are undoubtedly integrated into the treatment put in place by Clearview, including, contrary to what the company claims, the evaluation moment which can be said to coincide with the biometric comparison activity - carried out following the execution of a search by part of the user - and with the subsequent extraction of the profiles that can be associated with the image loaded into the system. This part of the process, which always belongs to Clearview, remains distinct from any further evaluation activity that can be carried out by the end user based on the results of the consultation and which, although related to the first in the sense required by art. 3.2.b, it cannot be superimposed on it, as instead objected by the company in its defense.

The overall assessment of the circumstances mentioned above leads to the inclusion of the conditions for the applicability of art. 3.2 of the Regulation and the discipline contained therein in the light of which the processing of personal data of Italian data subjects carried out by Clearview must therefore be assessed (see on this point also the decision of the German Supervisory Authority of the Land of Hamburg (decision 545 / 2020; 32.02-102) and of the Commission nationale de l'formatique et des liberté (CNIL, Decision n ° MED 2021-134 of 1st November 2021 issuing an order to comply to the company CLEARVIEW AI).

3.3. EXISTENCE OF THE JURISDICTION OF THE GUARANTOR

The processing carried out by Clearview qualifies as cross-border processing of personal data pursuant to art. 4, par. 1, no. 23 of the Regulation as capable of affecting data subjects in more than one Member State.

For this type of processing, where the owner has identified a single or main establishment in the European Union, the cooperation mechanism described in Articles 60 and following of the Regulations whose management is entrusted to the so-called Lead Supervisory Authority which coincides with the Supervisory Authority of the Member State in which the aforementioned establishment is located.

However, in cases in which the prerequisite for the operation of this mechanism is lacking, i.e. the presence in European territory of an establishment of the data controller, the latter will have to "interface with the supervisory authorities of each Member State in which it operates through of the designated representative "(see par. 3.3. of the" Guidelines on the Lead Supervisory Authority "adopted by the Article 29 Working Group on 13 December 2016, revised on 5 April 2017 and adopted

by the Personal Data Protection Committee on 25 May 2018).

In the present case, Clearview is a company based in the United States of America that has no plants in the territory of the European Union and, therefore, based on the provisions of art. 55, par. 1, of the Regulation, "each Supervisory Authority is competent to carry out the tasks assigned and to exercise the powers conferred on it in accordance with the (...) regulation in the territory of the respective Member State".

This provision is therefore suitable for establishing the competence of the Italian Data Protection Authority with regard to the assessment, with regard to its territory, of compliance with the European Regulation for the processing of personal data put in place by Clearview and to exercise the powers recognized to it. from art. 58 (see similar conclusion contained in paragraph IV of the decision of the Commission nationale de l'formatique et des liberté - CNIL, Decision n ° MED 2021-134 of 1st November 2021 issuing an order to comply to the company CLEARVIEW AI).

3.4 EXISTENCE OF A PROCESSING OF PERSONAL DATA AND GENERAL CONSIDERATIONS ON THE LAWFULNESS OF THE SAME

First of all, it is noted that a photographic image constitutes, pursuant to art. 4, par. 1, no. 1), of the Regulations, "personal data" to the extent that it allows the identification of a natural person (interested). The same provision specifies that "the person who can be identified, directly or indirectly, with particular reference to [...] one or more characteristic elements of his physical identity" is considered identifiable. With regard to photographic images, the Court of Justice of the European Union specifically intervened, stating that "the image of a person recorded by a camera constitutes personal data pursuant to the provision mentioned in the previous point [Art. 2.a of Directive 95/46, n.d.r.] if and insofar as it allows the data subject to be identified "(see judgment 11 December 2014, case C-212/13, par. 22).

Personal data obtained from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person that allow or confirm their unique identification, such as facial image, are defined as "biometric data", pursuant to art. 4, par. 1, no. 14), of the Regulation and, as such, subject to the higher protection regime provided for by art. 9 of the Regulations.

The difference between the two types of data is well defined by recital 51 of the Regulation, according to which "the processing of photographs should not systematically constitute the processing of particular categories of personal data, since they fall within the definition of biometric data only when they are processed through a specific technical device that allows the unique

identification or authentication of a natural person ".

As regards the concept of "treatment", it is noted that it is defined by art. 4, par. 1, no. 2), of the Regulation "any operation or set of operations [...] applied to personal data sets of personal data, such as collection, registration, organization, structuring, storage, adaptation or modification, 'extraction, consultation, use, communication by transmission, dissemination any other form of making available, comparison or interconnection, limitation, cancellation or destruction ".

As explained in paragraph 3.1, from the investigation conducted it emerged that Clearview has created a database of over 10 billion facial images which, collected on the Internet through web scraping techniques, are subjected to a biometric processing process with subsequent hashing for the purpose of indexing and research, by making the database available to third parties.

Given that the data in question can be classified as common and biometric data, it is necessary to analyze whether the activity carried out by the Company can be qualified as a treatment pursuant to and for the purposes of the Regulation.

In this regard, it seems first of all necessary to remember that the public availability of data on the Internet does not imply, by the mere fact of their public status, the legitimacy of their collection by third parties. In fact, any data that is published online undergoes this processing operation (in particular, the dissemination), on the basis of a legal basis and for specific and legitimate purposes established and pursued by the data controller who ordered its publication.

Even the cd. OSINT (open-source intelligence) techniques which consist in the collection and processing of information, including personal data, from freely available sources, such as the Internet and public data, can only be carried out against an adequate legal basis, as recently specified by the Guarantor European Union for the protection of personal data with reference to the aforementioned activity carried out by Europol (see EDPS Opinion on the possibility to use Clearview AI and similar services at Europol (Case 2020-0372)).

Likewise, it is noted that even the publication on the Internet of personal data by the subject to whom they refer, for example in the context of a social media network, does not in itself entail a sufficient condition to legitimize its free re-use by third parties.

If, in fact, it is true that the Regulation (and, therefore, in this case, the principle of purpose referred to in Article 5, paragraph 1, letter b), of the Regulation) does not apply to the processing of personal data carried out by a natural person for the exercise of activities of an exclusively personal or domestic nature (so-called household exemption, pursuant to Article 2, paragraph 2, letter c), of the Regulation), also with reference to line, it is also true that the exception must be interpreted strictly. As sanctioned by the Court of Justice of the European Union, the derogation "includes only activities that fall within the private or

family life of individuals, which clearly does not occur in the case of the processing of personal data consisting of their publication on the Internet in so as to make such data accessible to an indefinite number of people "(see judgment 6 November 2003, case C-101/01, par. 47). Therefore, it must also be considered that the publication of personal data by the interested party on social networks is bound to the mere purpose for which the interested party intended to make them public (for example, visibility in the context of a particular social network for sole purposes underlying the use of this SNS).

The correctness of the thesis is supported by the Article 29 Working Group, which clarified "that, even if they have been made accessible to the public, personal data continue to be considered as such and, consequently, for their processing they continue to be necessary adequate guarantees "(see Opinion 6/2014 - WP217) and, more recently, by the Personal Data Protection Committee, which established that" any communication of personal data constitutes a specific treatment for which the owner must have a legal basis among those referred to in Article 6 ", that" the transmission of films to third parties for purposes other than those for which the data were collected is possible pursuant to Article 6, paragraph 4 "and, finally, that "the third recipient will have to carry out its own legal analysis, in particular by identifying the legal basis of its processing pursuant to Article 6" (see Guidelines 3/2019 on the processing of personal data through video devices, version 2.0, January 29, 2020).

As regards, in particular, data scraping, this is a particular method of collection which takes place completely without the knowledge of the interested parties.

As mentioned, the possible public nature of the images is not sufficient to suggest that the interested parties can reasonably expect their use for facial recognition purposes, moreover by a private platform, not established in the Union and whose existence and activity most of those involved are oblivious.

In addition, web scraping activities are almost always prohibited by the managers of social networking services, through explicit clauses contained in the terms of service, so much so that, in this case, from press information, it emerged that some of the major providers of these services (Twitter, Youtube, LinkedIn) have sent a warning to Clearview to stop the collection of data that can be used to identify a person (cease and desist letter).

Based on the foregoing, it can be reasonably concluded that the collection of personal data freely available on the Internet using web scraping techniques constitutes a processing of personal data, which must be legitimized in one of the legal bases provided for by art. 6 of the Regulation.

Wanting to transpose this principle to the present case, it is believed that the web scraping of images put in place by the

Company integrates a personal data collection operation, which constitutes the processing of personal data.

In this case, however, the Company does not limit itself to collecting images from the Internet since, on such data, further processing operations are carried out, in this case, biometric processing and indexing by hashing. More specifically, the images depicting people's faces are subjected to further processing operations (vector representation) that transform the common image (personal data) into a facial image (biometric data).

Finally, the interconnection of the image data (common and biometric) referred to above with metadata collected, stored and associated with facial images, which, in turn, may contain personal data that reveal the racial origin or ethnicity, political opinions, religious or philosophical beliefs, trade union membership (the images could, in fact, be found on the websites of associations of faithful to a particular cult or members of a trade union or political party), circumstances that confirm the peculiarity of the treatments implemented by Clearview.

The analysis on the non-existence of the conditions of lawfulness for the processing of data outlined above on the basis of the structure of the Regulation and therefore from a personal data protection profile, will be analyzed in the next paragraphs.

Here, however, it seems necessary to anticipate some brief, broader considerations in relation to the legitimate profiles of the activity carried out by Clearview. As is known, in fact, in the European Union the debate on the legitimacy of the use of techniques that allow facial recognition is very lively and the attention threshold has risen following the approval, on 6 October 2021, by the Parliament of a resolution on artificial intelligence in criminal law and its use by police and judicial authorities in criminal matters. With this resolution it was proposed (to the European Commission) a permanent ban on the use of automatic analysis and / or recognition systems in public spaces not only of the face, but also of other human characteristics such as gait, fingerprints, DNA, voice and other biometric and behavioral signals. Furthermore, having acknowledged the different types of use of facial recognition, such as, but not limited to, verification / authentication (matching a live face to a photo in an identity document, e.g. smart edges), identification (finding a match between a photograph and an image database) and detection (finding faces in real time from sources such as closed circuit television and matching databases, e.g. real-time surveillance), each of which it has various implications for the protection of fundamental rights, the European Parliament requests that "the dissemination of facial recognition systems by law enforcement authorities be limited to clearly justified purposes in full compliance with the principles of proportionality and necessity and the law current". The European Parliament also reiterates that the use of facial recognition technologies must comply with the principles of minimization, accuracy,

purpose limitation and conservation, integrity and security.

On the basis of this recommendation, in Italy, with d.l. 139/2021, converted with amendments into l. 205/2021 (so-called "capacity decree"), a moratorium on biometric facial recognition systems in public places or places open to the public until 31 December 2023, with the exception, however, of the treatments carried out by the competent authorities for the purpose of prevention and repression of the offenses or execution of criminal sanctions pursuant to Legislative Decree 51/2018 (implementing Directive 2016/680, the so-called Law Enforcement Directive).

3.5 EXISTENCE OF OWNERSHIP

As set out in paragraph 2, the Company denied being the data controller, attributing the existence of this role only to the customers who use the platform. In particular, Clearview believes that it cannot be qualified as a data controller pursuant to and for the purposes of the Regulation as it limits itself to providing a research tool, the intended use of which, related to the identification of persons through facial recognition, would be the prerogative of customers, who would be responsible for acting in compliance with the applicable legislation in the reference area in which they operate. This assumption would be supported by the provisions of art. 25, par. 1, of the Regulation, in the part in which it provides that the owner, when determining the means of processing, must ensure that the parameters of the Regulation are respected. Consequently, it would be the customer's responsibility - and not Clearview's - to establish whether and how to use the search engine and therefore assume the role of data controller in relation to it.

The Guarantor considers this defensive line unfounded in fact and in law.

The definition of "data controller" set out in art. 4, par. 1, no. 7), of the Regulation establishes that those who determine the purposes and means of the processing must be considered as such and this can be done "individually or together with others". In the activity of collecting and processing images Clearview defines the methods and sources of the collection, creates the algorithm to be used for the creation of vectorial representations and establishes with which hash function to archive the images in this way also determining the parameters necessary for the indexing of information and its enrichment with useful metadata for greater effectiveness of the search results.

The company therefore uses its own means to carry out the collection of images and the subsequent transformation of them into biometric data, also having a proprietary database within which the information is stored and extracted as a result of the search performed by the user. The purpose pursued by Clearview is therefore to make available, for a fee, information, such

as images and metadata, useful to customers for the pursuit of different and additional purposes. Moreover, the European Data Protection Supervisor also reaches the same conclusion in the opinion cited above to the extent that it excludes that Clearview can qualify as a data controller acting on behalf of Europol (and Europol could not, therefore, make use of of its services pursuant to art.17, par.2, of EU Regulation 2016/7943) as Clearview sells a facial recognition service completely hosted and managed on its platform, independently deciding the purposes and essential elements of the means of services it offers (see EDPS Opinion on the possibility to use Clearview AI and similar services at Europol (Case 2020-0372), page 3).

The characteristics of the activity carried out by Clearview are already sufficient in themselves to argue that the same is a data controller. But these considerations also appear to be supported by the fact that, until March 2021, the privacy policy published on the Company's website contained a series of elements indisputably referable to the data controller, such as the indication of the legal basis of the processing, of the rights exercisable by the interested parties, as well as a specific e-mail address that can be used for requests for information and the exercise of rights by the interested parties pursuant to the Regulations. This address was also expressly attributed to the function of the data protection officer whose appointment is the responsibility of the data controller in accordance with the provisions of the Regulations governing the designation and attributions.

The fact that the customer who uses the platform pursues his own purposes is not relevant for the profiles that are of interest here. As clarified by the Personal Data Protection Committee, if a subject alone decides the purposes and methods of the operations that precede or are subsequent in the processing chain, that subject must be considered the sole owner of the previous or subsequent operation (see Lines Guide of the European Committee for the protection of personal data 07/2020 on the concepts of controller and processor in the GDPR, par.57). Therefore, the fact that Clearview's customers can pursue purposes other than those related to Clearview's business does not mislead, nor is it incompatible with the role of data controller of the latter.

3.6 VIOLATIONS FOUND

3.6.1 ART. 5, PAR. 1 LETT. A), B) AND E), OF THE REGULATION

In the first instance, the Office contested the violation of art. 5, par. 1, lett. a) of the Regulation, which provides for compliance with the principles of lawfulness, correctness and transparency in the processing of data towards the interested party.

On this point, Recital 39 of the Regulation expressly provides, among other things, that "the ways in which personal data concerning them are collected, used, consulted or otherwise processed should be transparent to individuals, as well as the

extent to which the personal are or will be processed. The principle of transparency requires that information and communications relating to the processing of such personal data are easily accessible and understandable and that simple and clear language is used […] ".

As represented above, in the present case, the interested parties have no contact with the Company, are not directly informed of the activity carried out by the same, nor are they recipients of any information even by consulting the Clearview website.

Secondly, the Office contested the violation of art. 5, par. 1, lett. b) of the Regulation, which provides for compliance with the purpose limitation principle which, even in the context of the balancing test between the legitimate interest of the owner and the rights and freedoms of the interested party (see below), represents one of the key factors to consider and which is embodied in the reasonable expectations of the interested parties (see Opinion 6/2014 - WP 217, page 47) that their images can be subjected to further processing.

In the present case, this principle does not seem to be considered integrated, even considering the absence of any relationship between the interested parties and the Company. In fact, the possible public nature of the images is not sufficient to suggest that the interested parties can reasonably expect their use for facial recognition purposes, moreover by a private platform, not established in the Union and whose existence and activities the most of those concerned are oblivious. On the other hand, and as already represented, the very circumstance of the public nature of the images does not automatically authorize Clearview to be able to legitimately reuse them freely, as the Company would like to suggest.

Finally, the Office contested the violation of art. 5, par. 1, lett. e) of the Regulation, which provides for compliance with the conservation principle.

There is no indication of any retention period either from the analysis of Clearview's privacy policy, or from the feedback received from the Company, incomplete results on this point, or from the information contained in the complaints submitted by the interested parties.

The Company has represented that the images are collected and stored with all the references (metadata) relating to the source and the moment in which the collection took place, thus creating a database, stratified and fed in a progressive and constant way, consisting of a series of information linked to a certain image over time. This aspect leads us to believe that such information is kept indefinitely and is deleted only at the express request of the interested parties. Among other things, this circumstance also denotes a contradiction with respect to what was declared by Clearview since the images being

processed are not always publicly available as images made private or deleted in their original source after the collection carried out by the Company also remain in the database. .

As represented above, it is believed that Clearview has expressly violated art. 5, par. 1 letter a), b) and e) of the Regulations. In particular, with reference to the obligations of transparency and lawfulness, art. 5, par. 1, lett. a) of the Regulations in light of the gravity, nature and impact of the individual specific violations of Articles 6, 9 and 12 to 14 of the Regulation (see EDPB binding decision 1/2021).

3.6.2. ART. 6 OF THE REGULATION

According to art. 6 of the Regulation, the processing of personal data is lawful if, and to the extent that at least one of the conditions listed in the same article is met.

In the present case, it being common ground that the consent of the interested parties has not been acquired and excluding the existence of the circumstances referred to in letters b), c), d) and e), it is necessary to analyze whether the legitimate interest of the owner can be considered to exist, legal basis implicitly invoked by the Company to the extent that it equates its activity to the processing carried out by Google Search in its indexing activity.

From this point of view, it seems first of all necessary to recall the general position taken on this point by the European Committee for the protection of personal data which ruled out that there may be "generalized authorization to reuse and further process personal data made accessible to the public to pursuant to article 7, letter f) [or, the legitimate interest of the current art. 6, lett. f] ", granting, at the most, that this circumstance can rise to a possible evaluation element in the balancing of interests (see Opinion 6/2014 - WP217).

In the present case, the legitimate interest of the company consists of a profit-making purpose in the face of a treatment that presents a particular intrusiveness in the private sphere of individuals, since it is essentially a collection of photographic data, associated with further links that they are suitable for detecting various aspects of individuals' private life. These data are also subjected to biometric processing and, finally, by the same declaration by the company, they relate to a particularly high number of subjects, to which a further element of delicacy must be added, that relating to the availability of images of minors on the Internet. , which are also subject to processing.

Considering the elements just represented, it is believed that the legitimate interest of the Company in free economic initiative can only decline with respect to the rights and freedoms of the interested parties, in particular the serious endangerment of the

right to privacy, the prohibition of being subjected to automated processing and the principle of non-discrimination inherent in the processing of personal data such as that carried out by the Company.

In conclusion, it is believed that Clearview cannot boast any valid legal basis on which to base the lawfulness of the processing of personal data put in place.

3.6.3 ART. 9 OF THE REGULATION

In the previous paragraphs it was highlighted how the treatment put in place by Clearview is not limited to a simple collection of data, but also consists of a further treatment that makes the images collected "biometric data" and, therefore, subject to the most stringent safeguards. of the art. 9 of the Regulations.

This article contemplates the legal regime concerning the categories of particular data, providing for a general prohibition of processing, subject to some exceptions. It is clear that the rationale of the provision is to provide for enhanced protection for certain categories of data by requiring, from an application point of view, a combination of the guarantees of art. 6 and the discipline of art. 9 of the Regulations. This also means that, to legitimize a processing activity, a data controller who processes particular categories of data can never invoke only a legal basis pursuant to art. 6, but must apply, in a cumulative manner, the provisions of art. 9 mentioned in order to ensure the relevant level of protection. In this sense, in the Guidelines no. 8/2020 "on the targeting of social media users", the Personal Data Protection Committee, which reiterated that "in addition to the conditions of Article 9 GDPR, the processing of particular categories of data must be based on a legal basis established in article 6 of the GDPR and be carried out in compliance with the fundamental principles referred to in article 5 of the GDPR ".

The cumulative application of the protections provided for by the aforementioned articles is also decisive for excluding interpretations that lead to support the possibility of processing particular categories of data, without respecting art. 6, in the presence of the exceptions referred to in art. 9. As reiterated, once again, by the Personal Data Protection Committee "it would be inappropriate to conclude, for example, that the fact that someone has made certain particular categories of data manifestly public pursuant to Article 8 [today art. 9 of the GDPR], paragraph 2, letter e), is (always in and of itself) a sufficient condition to allow any type of data processing, without carrying out a comparative test of the interests and rights at stake in accordance with article 7 [today art. 6 of the GDPR], letter f "(see Opinion 6/2014 - WP217).

In conclusion, for the reasons set out above, with reference to the processing of data put in place by Clearview, not only must there be no valid legal basis pursuant to art. 6 of the Regulation, but the general prohibition of processing particular categories

of data (with reference to biometric data) is also violated.

3.6.4. ARTT. 12, 13, 14 AND 15 OF THE REGULATION

The complaints submitted to the Authority were preceded by the forwarding to the data controller of preventive requests aimed at knowing which personal data concerning the interested parties were held by the Company, as well as, in some cases, the additional information indicated by art. 15 of the Regulation.

Complainants complained, in most cases, of the lack, delay or unsuitability of the feedback received and, therefore, a violation of art. 12 of the Regulations governing the procedures that the owner must observe, among other things, for communications resulting from the exercise of the rights provided for in Articles 15-22 by the interested party.

These circumstances then formed the subject of a notice to initiate proceedings pursuant to art. 166, paragraph 5, of the Code by the Authority as a result of which the following was found:

- with regard to Messrs. XX and XX, all the information required pursuant to art. 15 of the Regulation, but only a file containing the images extracted from the system and associated with the photograph sent by the interested parties together with the identity document was sent, referring, as regards the remaining requests, to a generic link to the privacy policy of the Company. The reply was also made within a period longer than the thirty days indicated in art. 12, par. 3, of the Regulations and only following several reminders sent by the interested parties;

- with regard to the complaint proposed by Mr. XX was instead detected the request for excess data, such as the identification document, in order to process the request for access formulated by the same.

The relations between the data controller and the interested parties, according to the indications provided by the Regulations, must be based on respect for transparency with regard to the information relating to the processing carried out, as well as with reference to the communications provided following the exercise of rights. In particular, based on the provisions of art. 12, par. 2, the data controller must facilitate the exercise of the rights of the interested party pursuant to articles 15 to 22 and this both with regard to the methods used to provide feedback and with regard to the timing thereof which, on the basis of the provisions from par. 3 of the same article, must be provided “without undue delay and, in any case, at the latest within one month of receipt of the request itself”, except for specifically regulated exceptions.

In some of the cases examined by the Authority - specifically XX and XX - the interested parties had to reiterate their requests for access several times before obtaining a response from Clearview and nevertheless the contact channels indicated on the

website of the Company (online form and e-mail address dedicated to privacy requests).

The methods made available by the Company for the exercise of the rights therefore proved neither easy nor clear, also by virtue of the overlapping of the channels indicated for making contact with it, and the terms provided for by the Regulations for providing reply to the interested parties, nor have the specific reasons required by art. 12, par. 4, of the Regulations for the possible extension of this term. In addition to this, Clearview, with the aim of evading access requests, has asked the interested parties for identification elements, such as the identity document, which are in excess of the pursued purpose given that, together with it, they have also been requested. to produce an image to which the data present in the owner's archive can be compared.

It is true, as objected by Clearview, that art. 12, par. 6, of the Regulation provides that "if the data controller has reasonable doubts about the identity of the natural person who submits the request referred to in articles 15 to 21, he may request further information necessary to confirm the identity of the interested party", but the provision requires precisely that such doubts are "reasonable" within the terms specified also in Recital 64. In the cases examined, the images requested from the interested parties, together with the other information provided, could be considered sufficient elements and, in any case, any further doubts could still be exceeded without necessarily having to request the attachment of a copy of the identity document.

The response to requests for access, with particular regard to the complaints proposed by Messrs. XX and XX, was also partial, since timely and transparent communication was not provided with reference to the categories of information provided for by art. 15, par. 1, of the Regulation which by reason of this appears to be violated.

The data controller, with a view to a relationship with interested parties based on fairness and transparency, is also required to provide some general information on the processing carried out, identified by Articles 13 and 14 of the Regulations, which must also be, in addition to being complete, also updated in order to take into account all the changes that occur over time.

As specified in paragraph 3.2, Clearview has made substantial changes to the information published on its site starting from March 20, 2021, or in an intermediate moment between the submission of the first two complaints (XX and XX) and the following two (XX and XX).

The privacy policy present on the site up to that date contained a series of indications relating to the processing of data carried out by Clearview which corresponded to the information contents indicated in Articles. 13 and 14 of the Regulation which, moreover, was expressly mentioned.

Already at the time, the information notice, although various aspects relating to the processing carried out, appeared to be partial as it lacked crucial elements, such as the specific indication of the legitimate interest pursued by the data controller or the specification of the term established for storage. of the data of the people whose images are held in the Clearview database

And this is with regard to the information to be provided with reference to personal data collected directly from the interested party (see Article 13 of the Regulation), such as those of users who request the service and those of those who exercise the rights of referred to in articles 15-22, which with reference to personal data collected through other sources and then re-processed by the company (see Article 14 of the Regulation).

Following the interventions put in place by various European supervisory authorities, the Company has, by its own statement made during the procedure, modified the information on the site by removing from it any reference to the European Regulation on data protection and eliminating also entire sections that integrated, in substance, the implementation of the provisions of the same (for example the explicit indication of the legal bases of the processing or the indication of the rights exercisable by the interested parties and which followed those referred to in articles 15-22 of the Regulation).

The current privacy policy continues to provide for the possibility for data subjects to know the information concerning them or to obtain its cancellation, but within the scope of the provisions applicable in California (see California Consumer Privacy Act (CCPA) and code Civil Code of California of 1798 cited in the disclosure) and therefore in terms other than those envisaged by the European Regulation.

For example, a limitation has been inserted - not provided for in European legislation or at least not in the manner indicated by the owner - to the number of access requests that the interested party can make within twelve months and which are established in the number of two.

There are also terms of response to requests that are different and longer than those contemplated in art. 12, par. 3, of the Regulations, providing that the impossibility for the owner to comply with them must simply be communicated to the interested party without indicating the specific conditions in the presence of which the slip may be deemed legitimate.

Finally, the exercise of the right of access is subject to the transmission by the interested party of an identity document, while in case of exercise of the right of cancellation, the possibility is provided for the holder not to satisfy it if, in the specific case, it occurs. one of the exceptions indicated by the provisions of the CCPA which are however not mentioned.

On the basis of what emerged, the violation of Articles 12, 15, 13 and 14 of the Regulations.

3.6.5. ART. 27 OF THE REGULATION

Art. 27 of the Regulation provides that, where art. 3, par. 2, the holder is required to designate in writing a representative in the European Union, who must be established in one of the Member States in which the data subjects whose data are processed in the context of the offer of goods and services are located or the whose behavior is monitored and who acts as an interlocutor, in particular of the supervisory authorities and data subjects, for all matters concerning the processing.

In the present case, the overall assessment of the circumstances set out above leads to consider the conditions of applicability of art. 3.2 of the Regulations; Clearview processes personal data of data subjects located in the Union and its processing activities are related to the provision of services to European users, as well as to the control of the behavior of individuals located in the territory of the Union.

The Company therefore has the obligation to designate, by written mandate, a representative in the territory of the European Union, instructing him to interact on its behalf with regard to the obligations deriving from the Regulations, also with regard to cooperation with the Supervisory Authority.

The omission integrates the violation of art. 27 of the Regulation.

3.6.6. ART. 22 OF THE REGULATION

In the act of initiating the procedure pursuant to art. 166 of the Code notified on 22 April 2021, the Office also contested the alleged violation of art. 22 of the Regulation, considering that the treatment put in place by the Company could imply the possibility of taking decisions, even if only partially automated, capable of producing significant effects with regard to the rights of the interested parties. From the investigation, no evidence emerged that could prove this violation. In fact, the Company has not provided any specific feedback on this profile and there are currently no technical system elements available that can corroborate the thesis of the existence of automated processing. It is also noted that art. 22 provides for the right not to undergo a decision based solely on automated processing but, from what emerged in the preliminary phase, this decision seems at the most to be able to be taken by customers of the service offered by Clearview and not by the Company, which has implemented and made its facial recognition system available to third parties.

From this point of view, it is therefore believed that there are no grounds for considering the violation of art. 22 of the Regulation.

CONCLUSIONS

In light of the assessments expressed above, therefore, most of the complaints of the Office notified with the initiation of the procedure are confirmed and the unlawfulness of the processing of personal data carried out by the Company is found, in violation of Articles 5, par. 1, lett. a), b) and e), 6, 9, 12, 13, 14, 15 and 27 of the Regulation.

The violation of the aforementioned provisions also makes the administrative sanction provided for by art. 83, par. 5, of the Regulation, pursuant to art. 58, par. 2, lett. i), and 83, par. 3, of the same Regulation and art. 166, paragraph 2, of the Code.

4. CORRECTIVE MEASURES

Art. 58, par. 2, provides for the Guarantor a series of corrective powers, of a prescriptive and sanctioning nature, to be exercised in the event that unlawful processing of personal data is ascertained.

Among these powers, art. 58, par. 2, lett. f), of the Regulation provides for the power to "impose a temporary or definitive limitation on processing, including the prohibition of processing".

Based on the foregoing, considering that the processing of personal data carried out by Clearview is carried out in violation of the principles of the Regulation, of the rules that these principles specify, in particular those on the legal basis, and of the rules relating to the rights of data subjects which represent the cornerstone of the Regulation, it is necessary, pursuant to art. 58, par. 2, lett. f), of the Regulation, to order a prohibition of processing, consisting in i) the prohibition of further collection, by means of web scraping techniques, of images and related metadata concerning persons who are in the Italian territory; ii) prohibition of any further operation of data processing, both common and biometric, processed by the Company through its facial recognition system relating to persons who are in the Italian territory.

Pursuant to art. 58, par. 2, lett. g), of the Regulation, it is also necessary, in order to make effective the protection of the numerous interested parties in the treatment put in place by the Company, to have a general order for the cancellation of the aforementioned data, without prejudice to the obligation to provide prompt response to requests for exercise of the rights referred to in Articles 15-22 of the Regulations that may have been received in the meantime by interested parties. In the latter cases, in order to facilitate the exercise of rights by the interested parties, the feedback must be provided in compliance with the times and methods set out in art. 12, par. 3 of the Regulation.

Pursuant to art. 58, par. 2, lett. d), of the Regulation, the Company is also ordered to designate, within thirty days of notification of the provision, a representative in the Italian territory who acts as an interlocutor, in addition to or in place of the owner, with

the interested parties in order to facilitate the exercise of rights.

Pursuant to art. 58, par. 1, lett. a), of the Regulation and 157 of the Code, the Company must communicate to this Authority, providing an adequately documented feedback, within thirty days from the notification of this provision, the initiatives undertaken in order to implement the aforementioned order pursuant to the aforementioned art. . 58, par. 2, lett. f), as well as any measures put in place to facilitate the exercise of the rights of the interested parties.

5. INJUNCTION ORDER FOR THE APPLICATION OF THE ADMINISTRATIVE PECUNIARY SANCTIONS AND ACCESSORY SANCTIONS

The Guarantor, pursuant to art. 58, par. 2, lett. i), and 83 of the Regulations as well as art. 166 of the Code, has the power to impose a pecuniary administrative sanction pursuant to Article 83, in addition to or in place of the other corrective measures provided for in the same paragraph.

In this case, the Guarantor adopts the injunction order with which it also disposes with regard to the application of the ancillary administrative sanction of its publication, in whole or in excerpt, on the website of the Guarantor pursuant to article 166, paragraph 7, of the Code "(Article 16, paragraph 1, of the Guarantor Regulation no. 1/2019).

In the present case, taking into account the provisions of art. 83, par. 3, of the Regulations, it is established first of all that the most serious violation must be recognized in the sanction provided for by art. 83, par. 5, which sets the maximum legal limit in the sum of 20 million euros or, for companies, in 4% of the annual worldwide turnover of the previous year, whichever is higher.

Pursuant to art. 83, par. 1 of the Regulation, the administrative sanction must be effective, proportionate and dissuasive in relation to the individual case.

Pursuant to art. 83, par. 2, of the Regulation, the decision on the determination and quantification of the amount of the sanction, in order for it to meet the characteristics of effectiveness, proportionality and dissuasiveness, must be taken taking into account a series of elements listed in par. 2, lett. a) -k).

To determine the amount of the sanction in the specific case, it is necessary to take into account the elements indicated in art. 83, par. 2, of the Regulation, which, in this case, can be considered in the following terms:

1. nature of the data processed;

2. severity and duration of the violation;

3. number of subjects involved;

4. degree of responsibility of the data controller;

5. measures adopted by the data controller;

6. degree of cooperation with the supervisory authority.

In relation to the nature of the data, it must be taken into account that the processing relates to particular categories of data, in particular biometric data, - probably also of minor subjects - with respect to which the regulatory framework for the protection of personal data provides a higher level of protection.

With regard to the severity of the violations, it is noted that Clearview has violated Articles 6 and 9 of the Regulation, which represent the conditions of lawfulness and therefore the fundamental requirements for processing pursuant to the Regulation.

The unlawful processing of biometric data for facial recognition purposes must also be considered a very serious violation given the position taken by the European and Italian legislators regarding the illegality of this type of activity which involves mass surveillance. Furthermore, the violations do not constitute an isolated event as the processing carried out by the Company takes place in a systematic manner and has continued even after the service has no longer been offered to customers established in the European Union.

As for the number of subjects involved, the data cannot be quantified with precision, but considering that the collection of images took place "trawling" with web scraping techniques, it is reasonable to assume that it involves a very high number of interested parties, potentially all natural persons that are located in Italy and are present on the Internet, through accounts on social network services or other publicly accessible sources that portray them for personal or professional reasons.

The degree of responsibility of the owner is very high as the illegal processing activity has not only continued despite the intervention of numerous personal data protection authorities (European and non-European), but also because its legitimacy is strongly claimed through the denial of European, and in particular Italian, jurisdiction.

Despite the aforementioned interventions by other authorities and the objections raised by the Guarantor with the two acts of initiation of the procedure pursuant to art. 166 of the Code, the Company has not adopted any measures to conform its activity to the Regulation and indeed has decided to modify, starting from March 2021, its privacy policy by eliminating any reference to it.

Lastly, with reference to the degree of cooperation, it is noted that the Company, despite having formally acknowledged both

the request for information and the two disputes pursuant to art. 166 of the Code, on the merits supported and reiterated the inapplicability of the Regulation to the processing activity put in place and did not provide timely feedback to individual requests.

The only mitigating factor that is noted is the lack of previous violations committed by the data controller or previous measures pursuant to art. 58 of the Regulation.

Due to the aforementioned elements, assessed as a whole, in the absence of data relating to the total annual worldwide turnover of the Company's previous year, it is considered to determine, pursuant to art. 83, par. 3, of the Regulations, the amount of the pecuniary sanction for the violation of Articles 5, par. 1, lett. a), b) and e), 6, 9, 12, 13, 14, 15 and 27, to an extent equal to the maximum legal limit provided for by art. 83, par. 5, of the Regulation, considered the most serious violation, i.e. a total of 20 million euros (in detail, 3.8 million euros for each violation of articles 5, 6 and 9 of the Regulation; 2 million euros for each violation of articles 12, 13, 14 and 15 of the Regulations; 600,000 thousand euros for the violation of Article 27 of the Regulations).

This administrative pecuniary sanction is deemed, pursuant to art. 83, par. 1, of the Regulation, effective, proportionate and dissuasive.

Taking into account the particular delicacy of the data processed, it is also believed that the ancillary sanction of the publication on the website of the Guarantor of this provision, provided for by art. 166, paragraph 7 of the Code and art. 16 of the Guarantor Regulation n. 1/2019.

Please note that pursuant to art. 170 of the Code, anyone who, being required to do so, does not comply with this provision of prohibition of processing is punished with imprisonment from three months to two years and who, in the event of non-compliance with the same provision, the sanction referred to in administrative office is also applied. to art. 83, par. 5, lett. e), of the Regulation.

Finally, it is believed that the conditions set out in art. 17 of Regulation no. 1/2019 concerning internal procedures with external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor, for the annotation of the violations found here in the internal register of the Authority, provided for by art. 57, par. 1, lett. u) of the Regulations.

WHEREAS, THE GUARANTOR

pursuant to art. 57, par. 1, lett. f), of the Regulations, declares unlawful the processing described in the terms set out in the

motivation by Clearview AI, with registered office at 214 W 29th St, 2nd floor, New York City, NY, 10001, U.S.A. and consequently:

a) pursuant to art. 58, par. 2, lett. f), of the Regulation, prohibits the continuation of the processing and further collection, by means of web scraping techniques, of images and related metadata concerning persons who are in the Italian territory and the prohibition of any further data processing operation, common and biometric, processed by the Company through its own facial recognition system, in relation to people who are in the Italian territory;

b) pursuant to art. 58, par. 2, lett. g), of the Regulations, orders the deletion of data, both common and biometric, processed by the Company through its facial recognition system relating to people who are in the Italian territory, without prejudice to the obligation to provide prompt response to requests for the exercise of rights referred to in Articles 15-22 of the Regulations that were eventually received by interested parties in compliance with art. 12, par. 3, of the Regulation.

c) pursuant to art. 58, par. 2, lett. d), of the Regulation orders the Company, within thirty days of notification of the provision, to designate a representative in the territory of the European Union who acts as an interlocutor, in addition to or in place of the owner, with the interested parties in order to facilitate its exercise. rights.

ORDER

a Clearview AI, located at 214 W 29th St, 2nd floor, New York City, NY, 10001, U.S.A. to pay the sum of twenty million euros as a pecuniary administrative sanction for the violations indicated in the motivation, representing that the offender, pursuant to art. 166, paragraph 8, of the Code, has the right to settle the dispute, with the fulfillment of the prescribed requirements and the payment, within sixty days, of an amount equal to half of the sanction imposed.

INJUNCES

to the aforementioned Company, in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, to pay the sum of twenty million euros, according to the methods indicated in the annex, within 30 days of notification of this provision, under penalty of the adoption of the consequent executive acts pursuant to art. 27 of the law n. 689/1981.

HAS

a) pursuant to art. 17 of the Guarantor Regulation n. 1/2019, the annotation in the internal register of the Authority, provided for by art. 57, par. 1, lett. u) of the Regulations, violations and measures adopted;

b) pursuant to art. 166, paragraph 7, of the Code, the full publication of this provision on the website of the Guarantor.

The Guarantor, pursuant to art. 58, par. 1, lett. a) of the Regulations invites the data controller to communicate within 30 days from the date of receipt of this provision, which initiatives have been undertaken in order to implement the provisions of this provision, providing adequately documented feedback. Please note that failure to respond to the request pursuant to art. 58 is punished with the administrative sanction pursuant to art. 83, par. 5, lett. e), of the Regulation.

Pursuant to art. 78 of the Regulation, as well as art. 152 of the Code and 10 of the legislative decree 1 September 2011, n. 150, opposition to this provision may be filed with the ordinary judicial authority, with an appeal filed with the ordinary court of the place where the data controller is resident, or, alternatively, to the court of the place of residence of the person concerned. , within thirty days from the date of communication of the provision itself, or sixty days if the applicant resides abroad.

Rome, February 10, 2022

PRESIDENT

Stanzione

THE RAPPORTEUR

Peel

THE SECRETARY GENERAL

Mattei