[doc. web no. 9446730]

Injunction against Cavauto s.r.l. - March 26, 2020

Register of measures

no. 65 of 26 March 2020

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, in the presence of Dr. Antonello Soro, president, of dr. Augusta Iannini, vice president, of dr. Giovanna Bianchi Clerici and of prof. Licia Califano, members, and of dr. Giuseppe Busia, general secretary;

HAVING REGARD TO Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, as well as on the free circulation of such data and repealing Directive 95/46 /CE (General Data Protection Regulation, hereinafter "Regulation");

HAVING REGARD TO the Code regarding the protection of personal data, laying down provisions for the adaptation of national legislation to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, relating to the protection of individuals with regard to processing of personal data, as well as the free movement of such data and repealing Directive 95/46/EC (Legislative Decree June 30, 2003, No. 196, as amended by Legislative Decree August 10, 2018, No. 101, hereinafter "Code");

HAVING REGARD to the "Guidelines for e-mail and the Internet", adopted with provision no. 13 of 1 March 2007 (published in the Official Journal of 10 March 2007, n. 58);

HAVING REGARD to the complaint presented to the Guarantor pursuant to article 77 of the Regulation by XX concerning the processing of personal data relating to the data subject carried out by Cavauto s.r.l.;

HAVING EXAMINED the documentation in the deeds;

HAVING REGARD TO the observations made by the general secretary pursuant to art. 15 of the Guarantor's regulation n. 1/2000;

SPEAKER Dr. Antonello Soro;

WHEREAS

1. The complaint against the company and the preliminary investigation.

1.1 With a complaint dated 24 July 2018, Ms XX (represented and defended by lawyer XX) asked the Authority to order the

blocking or prohibition of the processing of personal data, deemed unlawful, carried out by Cavauto s.r.l. (hereinafter: the company) through access to the browsing history and other data collected during the employment relationship also through the company PC, subsequently used in a disciplinary proceeding against the complainant which ended with the dismissal (cf. dispute disciplinary dated 29.5.2018 and dismissal letter dated 5.6.2018, attached to the complaint). The complaint also requests that the company be ordered to satisfy "the [...] right of access [...] to the PC supplied until the date of termination of the employment relationship in order to identify and obtain the deletion of files containing personal data […]; to the e-mail archive of the address customercare@cavauto.com in order to identify and obtain the cancellation of e-mails with personal content [...]; to company premises in order to obtain the recovery of all personal documents kept in paper form in the desk and chest of drawers used by him; to the pages of the personal diary retained by the company, in order to identify and obtain the destruction of personal content" (see complaint cited, p. 6-7).

According to what is represented, these processing operations  and in particular access to the PC supplied "for exclusive use [...] and equipped with a password" for the performance of one's duties, which also contains data "of a personal and family nature"  would be occurred "without [the complainant] being notified or even present" (cf. cited complaint, p. 3). Furthermore, the company did not inform the person concerned about "the prohibition to use the company PC and the internet for non-work purposes" or to consult "the personal e-mail address which she also used for work reasons", nor of the possibility for the employer to work to carry out checks, specifying the type, on the correct use of company tools.

1.2. The company, in response to the request for elements (of 24.9.2018) formulated by the Office, stated that:

to. the "PC assigned to the former employee [...] was equipped with a single but company password, so as to allow access only to the [complainant] and, if necessary, to Mr. XX, in his capacity as direct superior";

b. access to the complainant's PC "was limited [...] to detecting the history of the sites visited by the worker and was not extended to other data, neither to the customarecare@cavauto account, nor to the personal gmail account";

c. access to the PC was carried out "in the context of defensive investigations, [...] by Mr. XX, legal representative of the company, in the presence of the external technician of the same [...]";

d. the PC used by the complainant "used the Google Chrome browser which records the history of navigation data, as there is no company server on which such data is recorded [...]";

And. the company "provided oral and written information upon assignment of the work tools subsequently made known through

publication of the internal regulation on the use of electronic tools on the virtual bulletin board available on the company intranet";

f. "for defensive purposes it was not possible to follow up on the request for access by the [complainant] to the PC and to the data contained therein, given that the electronic instrument after inspection by the legal representative [...] was sealed and is no longer used by anyone, since it constitutes a source of evidence in court".

1.3. With reply notes dated 19 December 2018 and 1 March 2019, the complainant reiterated the requests already made to the Authority, stating  among other things  that "the use [...] of the company PC has always taken place in compliance with the directives received and any use other than strictly work has always been [...] known and tolerated" as it did not affect work performance (note 12.19.2018, p. 3). Furthermore, he complained that the regulation referred to by the company, concerning the use of corporate tools and the possible related controls, bears a date (21.5.2018) after the one in which access to the complainant's PC was made (16.5. 2018) (note 1.3.2019, p. 4-5).

1.4. On 17 May 2019, the Office carried out, pursuant to art. 166, paragraph 5, of the Code, the notification to the company of the alleged violations of the Regulation found. With a note dated June 16, 2019, the company, represented and defended by lawyers XX and XX, represented that:

to. the assignment to the (former) employee of a password to access the PC shared with the legal representative was assessed as an "adequate" measure, both because "no personal data should have been transmitted, stored or otherwise processed via the company PC , as required by company practice, by the instructions provided upon hiring and by company policies which prohibited the use of electronic work tools for private purposes" and because the employee had not been assigned a "personal company" account ( note 16.6.2019, p. 2);

b. "oral and written information was provided upon assignment of the work tools subsequently disclosed through publication of the internal regulations [...] on the virtual bulletin board available on the company intranet" (note cit., p. 2);

c. "a mere list of Internet sites [cannot] be considered «personal data»” (note cit., p. 3);

d. "even if we want to qualify Internet traffic data as "personal data", the legal basis underlying the processing [...] must be found in the "pursuit of a legitimate interest" of the owner in accordance with art. 6.1 letter f) and recital 47 of the Regulation" (note cit., p. 3);

And. in response to the requests for access made by the complainant, the company, in accordance with the provisions of the

law, delivered a USB stick as well as the agenda, even if deprived of some pages, while in relation to all the data present in the PC and the deleted pages from the agenda "was unable to follow up on these requests for «defensive» reasons", in line with the provisions of art. 2-undecies, lett. e) of the Code; in fact, at the time of the presentation of the application "there was already a dispute between the parties" which then resulted in the appeal against the dismissal; the existence of "conditions that legitimized a partial limitation of the right of access" was communicated, in accordance with the provisions of art. 2-undecies, paragraph 3, of the Code, with a note from the company's lawyer dated 10 July 2018 (cited note, p. 5);

f. the regulations in force on remote controls are not applicable, both because "the mere knowledge of internet traffic [...] does not constitute "personal data"", and because "in the present case [in question] control [...] "defensive » [...] outside the scope of applicability of art. 4 of the workers' statute" (note cit., p. 5-6).

1.5. During the hearing requested by the company and held on 24 July 2019, the legal representative underlined that the behavior deemed "incorrect" by the employee occurred in contrast with the provisions (also) of the internal company Regulations dated 17 October 2017, provided in copy . The company also deemed that it had acted legitimately in its control activity also on the basis of what was published on a site connected to a specialized newspaper (Il Sole 24 Ore, 29.5.2018, "Employee PCs are controllable").

2. The outcome of the investigation.

As a result of the examination of the declarations made to the Authority during the proceedings as well as of the documentation acquired, it appears that the company, as owner, has carried out some operations of processing of personal data referring to the complainant − in a period of time immediately preceding and immediately following the application in national law, starting from 25 May 2018, of Regulation (EU) 2016/679 − which are not compliant with the regulations on the protection of personal data, in the terms described below.

2.1. Given that, unless the fact constitutes a more serious offence, whoever, in a proceeding before the Guarantor, falsely declares or certifies news or circumstances or produces false deeds or documents is liable pursuant to art. 168 of the Code "False declarations to the Guarantor and interruption of the execution of the duties or the exercise of the powers of the Guarantor", on the merits it emerged that the company, in the person of the legal representative, on 16 May 2018 (as certified by the same owner in the disciplinary dispute of 29.5.2018) accessed the PC provided for use by the complainant by extracting the history of Internet access made available by Google Chrome. Access by the employer was allowed by sharing the access

password between the complainant and the legal representative of the company. At present, it does not appear that the company has agreed to change the described password management practice.

This sharing is in contrast with the obligation to adopt security measures aimed at ensuring "a minimum level of protection of personal data" (see art. 33, of the legislative decree 30.6.2003, n. 196, Code on the matter of protection of personal data, text in force at the material time).

In fact, within the context of IT authentication systems, the authentication credentials assigned to the persons in charge consist, at least, of an identification code associated with a keyword known exclusively by the interested party. In place of the password, having regard to the concrete nature of the information contained in the system, devices placed in the exclusive availability of the interested party can be delivered (see what has already been established in the Technical Regulations on minimum security measures, rules 1-11, Annex B of the Code, text prior to the amendments made with Legislative Decree No. 101/2018).

This principle is included in the art. 32 of the Regulation, according to which the data controller, in order to guarantee the confidentiality and integrity of the IT systems, must adopt "adequate technical and organizational measures to guarantee a level of security appropriate to the risk". Furthermore, based on art. 5, par. 1, lit. f) of the Regulation, the owner must guarantee "adequate security of personal data" by applying the principles of "integrity and confidentiality" to the treatments carried out.

2.2. It also appears that access to the PC assigned to the complainant, in the absence of the same, took place without the interested party having been provided with suitable information. In fact, the individual disclosure, signed by the complainant on 10.14.2016, does not contain any indication on the use of e-mail, internet access and other work tools, nor on the type of controls that the employer reserves to activate.

As for the alleged information which, by admission of the same complainant (see letter dated June 4, 2018 in the file), appears to have been given informally, no evidence was provided by the company that it was exhaustive and in any case compliant with the multiple criteria expressed by the jurisprudence of the Guarantor (see for all the provision containing the "Guidelines of the Guarantor for e-mail and Internet" (adopted by the Authority on 1 March 2007 and published in the Official Gazette no. 58 of 10 March 2007). On the other hand it is noted that the documents containing the "Internal Regulations" relating (also) to the use of work tools adopted by the company, both in the version dated 10.17.2017 (delivered to the Authority only on 07.24.2019) and in the one dated 21.5.2018 (subsequent, in any case, to the facts which are the subject of the complaint), are

without signature and elements suitable to indicate the certain date.

Given this, in any case, the provision contained in the text of the aforementioned regulation in relation to the controls that can be activated on Internet browsing ("Internet browsing is prohibited for reasons other than those functional to the work activity itself; for the purposes of protecting the company assets, the internet connections of each client will be checked regularly in compliance with privacy regulations"), where it seems to provide for "regular" checks (without specifying the methods) on internet connections does not appear to comply with the principles of lawfulness and proportionality (see art. 5, paragraph 1, letters a) and c), of the Regulation; v. also "Guidelines for e-mail and internet", cited in the introduction, points 5.2. and 6.1.).

The data controller, therefore, has not fulfilled the obligation to provide prior information to the interested party regarding the essential characteristics of the treatments carried out (see article 13 of the Code, text in force at the time of access to the PC of the complainant ; the obligation to provide the information to the interested party is, under current legislation, established by Article 13 of the Regulation). In the context of the employment relationship, the obligation to inform the employee is also an expression of the general principle of correctness of the treatments (see 11, paragraph 1, letter a), of the Code text in force at the time of access to the PC of the claimant; principle merged into art. 5, par. 1, lit. a) of the Regulation; v. European Court of Human Rights, Grand Chamber, case of Bărbulescu v. Romania, Application no. 61496/08, 5 September 2017, spec. no. 140).

The provisions of art. 6 of the Regulation on legitimation criteria.

2.3. The data controller only partially met the access requests presented by the complainant (on 4 and 12 July 2018), refusing access to the data contained in the PC with the exception of those transferred to a USB stick and to some pages of the diary used by the complainant removed before delivery as well as the request to verify the existence of further personal documents within the room assigned to the complainant at the time.

The limitations on the exercise of rights, including that of access, have been governed, pursuant to art. 23 of the Regulation, by art. 2-undecies of the Code which entered into force on a date following the presentation of the request and the acknowledgment note by the data controller. However, in application of general principles and in compliance with the provisions of the previous Code, on the basis of the aforementioned law in force, the right of access can be limited by the owner only in the presence of one of the specific conditions indicated and provided that reasoned communication is given to the interested party . In the present case, in rejecting the request for access, specific reasons for the protection of the rights referred to the data specifically object of the request were not indicated. In fact, with the note dated 10.7.2018 (Annex 5,

company note 26.10.2018), the complainant was informed that the company computer and e-mail box "should not contain «files containing personal data, saved in the memory of the PC itself, and of the internet history attributable to [...] private life»" and that "the personal assets of the worker [...] have all been returned". Nothing, therefore, has been represented in relation to a possible postponement or limitation or exclusion of the right of access asserted against the owner.

3. Conclusions: illegality of the treatment. Corrective measures pursuant to art. 58, par. 2, Regulation.

For the aforementioned reasons, the processing of personal data carried out by the company is certainly illegal pursuant to articles 5 and 6, of the Regulation, and also constitutes a violation of art. 4 law n. 300/1970 as modified by the d. lgs. no. 151/2015. Further profiles of illegality were ascertained in relation to the violation of the security measures, governed at the material time by art. 33 of the Code in force at the time of access to the complainant's PC. Also considering that the company has not changed its policy in this regard, the art. 32 of the Regulation. The treatment also took place in violation of the art. 13 of the Code in force at the time of access to the complainant's PC in the terms set out above. Also considering that the company has not modified its information documents on this point, art. 13 of the Regulation. The unsuitable and partial response provided to the request for access in relation to art. 23 of the Regulation.

On the other hand, here it is not necessary to carry out an assessment of the legitimacy of the allegedly "defensive" check carried out by the company following the detection of the non-compliance with official duties by the complainant, as this question may, if anything, be the subject of scrutiny by the judicial authority.

In the light of the above, given the corrective powers attributed by art. 58, par. 2 of the Regulation, in the light of the circumstances of the specific case:

- the further processing of data extracted from Internet history is prohibited (Article 58, paragraph 2, letter f) of the Regulation), except for their conservation for the exclusive purpose of protecting rights in court − in relation to the proceedings pending before the ordinary judicial authority − taking into account that, pursuant to art. 160-bis of the Code, "The validity, effectiveness and usability in judicial proceedings of deeds, documents and provisions based on the processing of personal data that does not comply with the provisions of the law or the Regulations remain governed by the pertinent procedural provisions";
- the company is ordered to satisfy the request for access to the complainant's data (Article 58, paragraph 2, letter c) of the Regulation) contained in the company PC as well as to other personal data currently held (also, possibly, in the account customercare@cavauto.com, even if it is a non-individualized address), with particular reference to the pages of the agenda

held by the company at the time of return and to any data contained in additional documents, if applicable, present in the spaces and furnishings previously assigned to the employee (see the complainant's reply note of 1.3.2019);

- the company is ordered to conform its treatments to the provisions of art. 32 of the Regulation on security measures (art. 58, par. 2, letter d) Regulation);

- the company is ordered to bring its processing into line with the Regulations, also with reference to the provisions of the internal regulation, providing for measures aimed at preventing the risk of improper or promiscuous use of the company's PCs and systems, also with reference to the Internet browsing of employees, in any case refraining from excessively general provisions relating to the methods of controls;

- in addition to the corrective measures, a pecuniary administrative sanction is ordered pursuant to art. 83 of the Regulation, commensurate with the circumstances of the specific case (Article 58, paragraph 2, letter i) of the Regulation).

4. Injunction order.

Pursuant to art. 58, par. 2, lit. i) of the Regulation and of the art. 166, paragraphs 3 and 7 of the Code, the Guarantor orders the application of the pecuniary administrative sanction provided for by art. 83, par. 5, letter. a) of the Regulation, by adopting an injunction order (art. 18, l. 11.24.1981, n. 689), in relation to the processing of personal data referring to the complainant carried out by the company through the methods of access to the browsing history on the Internet, as well as through the unsuitable and partial response provided to the access request, in the terms set out above, in relation to articles 5, 6, 13, 32 and 88 of the Regulation, following the outcome of the procedure pursuant to art. 166, paragraph 5 carried out jointly with the data controller (see previous points 1.4. and 1.5).

Considering it necessary to apply paragraph 3 of the art. 83 of the Regulation where it provides that "If, in relation to the same treatment or related treatments, a data controller [...] violates, with willful misconduct or negligence, various provisions of this regulation, the total amount of the pecuniary administrative sanction does not exceed amount specified for the most serious violation", considering that the ascertained violations of art. 5 of the Regulation, are to be considered more serious, as they relate to the non-compliance with a plurality of principles of a general nature applicable to the processing of personal data, the total amount of the fine is calculated so as not to exceed the maximum prescribed for the aforementioned violation.

Consequently, the sanction provided for by art. 83, par. 5, letter. a) and c) of the Regulation, which fixes the statutory maximum in the sum of 20 million euros or, for companies, in 4% of the annual worldwide turnover of the previous year, if

higher.

With reference to the elements listed by art. 83, par. 2 of the Regulation for the purposes of applying the pecuniary administrative sanction and the relative quantification, taking into account that the sanction must "in any case [be] effective, proportionate and dissuasive" (Article 83, paragraph 1 of the Regulation), it is represented that In the present case, the following circumstances were considered:

a) in relation to the nature, gravity and duration of the violation, the nature of the violation which concerned the general principles of processing was considered relevant; the violations also concerned the provisions on the exercise of rights, on security measures, on the legal basis of the processing and on information;

b) with reference to the intentional or negligent nature of the violation and the degree of responsibility of the owner, the negligent conduct of the company and the degree of responsibility of the same was taken into consideration which did not comply with the data protection regulations in relation to a plurality of provisions;

c) the company has fully and actively cooperated with the Authority during the proceeding;

e) the absence of specific precedents (relating to the same type of treatment) against the company.

It is also believed that they assume relevance in the present case, taking into account the aforementioned principles of effectiveness, proportionality and dissuasiveness with which the Authority must comply in determining the amount of the fine (Article 83, paragraph 1, of the Regulation), in firstly, the economic conditions of the offender, determined on the basis of the revenues achieved by the company with reference to the financial statements for the year 2018. It is also believed necessary to take into account the complex of corrective measures actually adopted against the company. Lastly, account is taken of the statutory sanction established, in the previous regime, for the corresponding administrative offenses and of the extent of the sanctions imposed in similar cases.

In the light of the elements indicated above and the assessments made, it is believed, in the present case, to apply against Cavauto s.r.l. the administrative sanction of the payment of a sum equal to 10,000.00 (ten thousand) euros.

In this context, it is also believed, in consideration of the nature and seriousness of the violations ascertained, that pursuant to art. 166, paragraph 7, of the Code and of the art. 16, paragraph 1, of the Guarantor Regulation n. 1/2019, this provision must be published on the Guarantor's website.

It is also believed that the conditions pursuant to art. 17 of Regulation no. 1/2019 concerning internal procedures having

external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

It is recalled that, pursuant to article 170 of the Code, anyone who fails to comply with this prohibition provision is punished with imprisonment from three months to two years; in any case, the sanction referred to in art. can be applied in the administrative office. 83, par. 5, letter. e), of the Regulation.

ALL THAT BEING CONSIDERED, THE GUARANTOR

pursuant to articles 57, par. 1, lit. f) and 58, par. 2, lit. c), d), f) and i) of the Regulation:

1. orders against Cavauto s.r.l. the limitation of the processing of data extracted from Internet chronology (Article 58, paragraph 2, letter f) of the Regulation), to the sole conservation for the exclusive purpose of protecting rights in court, within the limits set forth in Article 160-bis of the Code;

2. orders Cavauto s.r.l. to satisfy the request for access to the data contained in the company PC as well as to other personal data currently held, with particular reference to the pages of the agenda retained by the company at the time of return (Article 58, paragraph 2, letter c) regulation);

3. orders Cavauto s.r.l. to conform their treatments to the provisions of art. 32 of the Regulation on security measures, within 60 days of receipt of this provision (Article 58, paragraph 2, letter d) of the Regulation);

4. orders Cavauto s.r.l. to conform its internal policy to the Regulation by providing for measures aimed at preventing the risk of improper or promiscuous use of company PCs and systems, also with reference to employees' Internet browsing, within 60 days of receipt of this provision (art. 58, paragraph 2, letter d) Regulation);

5. inflicts on Cavauto s.r.l., in addition to the corrective measures, the pecuniary administrative sanction provided for by art. 83, par. 5, letter. a) of the Regulations, ordering and simultaneously enjoining the aforesaid offender to pay the sum of 10,000.00 (ten thousand) euros according to the methods indicated in the attachment, within 30 days of notification of this provision, under penalty of the adoption of the consequent executive deeds norm of art. 27 of the law n. 689/1981; this without prejudice to the faculty for Cavauto s.r.l. to settle the dispute by paying an amount equal to half of the fine imposed within 30 days from the date of notification of this provision, pursuant to art. 166, paragraph 8 of the Code;

6. has, pursuant to art. 166, paragraph 7, of the Code, the publication of this provision/injunction order on the Guarantor's website;

7. believes that the conditions pursuant to art. 17 of Regulation no. 1/2019 concerning internal procedures having external

relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor;

8. requests to Cavauto s.r.l. to communicate which initiatives have been undertaken in order to implement the provisions of this provision and in any case to provide adequately documented feedback pursuant to art. 157 of the Code, within 90 days from the date of notification of this provision; any failure to reply may result in the application of the administrative sanction provided for by art. 83, par. 5, letter. e) of the Regulation.

Pursuant to art. 78 of the Regulation, as well as articles 152 of the Code and 10 of Legislative Decree no. 150/2011, opposition to this provision may be lodged with the ordinary judicial authority, with an appeal lodged with the ordinary court of the place where the data controller has his residence, within the term of thirty days from the date of communication of the provision itself or sixty days if the appellant resides abroad.

Rome, 26 March 2020

PRESIDENT

Soro

THE SPEAKER

Soro

THE SECRETARY GENERAL

Busia