[doc. web n. 8429116]

Injunction order against Trivenet s.r.l. - January 25, 2018

Record of measures

n. 32 of 25 January 2018

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

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

NOTING that the special privacy unit of the Finance Police, in execution of the request for information no. 21868/97157 of 27 July 2015, formulated pursuant to art. 157 of Legislative Decree 30 June 2003, n. 196, containing the Code regarding the protection of personal data (hereinafter "Code"), carried out the investigations at Trivenet s.r.l., operating as a telephone and telematic operator, based in Galleria Veneta (PD), Viale Europa n . 20, P.I. 03350610287, formalized in the minutes of operations carried out on 21 and 22 October 2015, aimed at verifying compliance with the legislation on the protection of personal data and with the provisions of the Guarantor in the provision concerning "Security of telephone and electronic traffic data "dated 17.01.2008 (in www.garanteprivacy.it, web doc. no. 1482111), supplemented by the provision of 24.07.2008, containing" Regulatory transposition on telephone and telematic traffic data "(in www.garanteprivacy.it , web doc. no. 1538237). During the investigations carried out, it was found that the Company, as the data controller pursuant to art. 28 of the Code:

- has kept the data relating to unanswered calls for a period of time exceeding that of thirty days provided for by art. 132, paragraph 1-bis, of the Code;
- kept the traffic data for billing purposes on the BDC server, in the folder called Area Billing, for a period exceeding six months, in violation of the provisions of art. 123 of the Code;
- kept the telephone and telematic traffic data for the purpose of ascertaining and repressing crimes beyond the terms of 24 months and 12 months respectively, provided for by art. 132 of the Code;
- has not observed the measures and precautions prescribed by the Guarantor pursuant to art. 17 of the Code, since it has carried out a processing of telephone and electronic traffic data for the purpose of ascertaining and repressing crimes without adopting the measures prescribed by the Guarantor with the provision of 17 January 2008 (in the Official Gazette of 5

February 2008 no.30, and on the website www.garanteprivacy.it, in web doc. no.1482111), modified and integrated by the subsequent provision of 24 July 2008 regarding the retention of telephone and electronic traffic data (in the Official Gazette of 13 August 2008 no.189, doc web n. 1538224), with particular reference to the biometric recognition procedure required for the control of selected access areas, the strong authentication procedure, the cryptographic techniques required to protect the traffic data processed for legal purposes, the internal controls aimed at verifying the effective cancellation of the data after the retention periods have elapsed;

TAKING NOTE of the documentation sent by the Company on November 6, 2015, to dissolve the reservations formulated during the inspections, with which it declared that it had initiated a series of actions aimed at remedying the critical issues found during the inspection visit and, in in particular, to have carried out the deletion of data that were stored beyond the terms of the law;

GIVEN the minutes n. 112 of 3 December 2015, which is understood to be fully referred to here, with which Trivenet s.r.l., as the data controller, in the person of the pro-tempore legal representative, was charged with the administrative violation provided for by art. 162-bis of the Code, in relation to art. 132, paragraph 1-bis, informing you of the right to make a reduced payment pursuant to art. 16 of the law of 24 November 1981 n. 689;

NOTING that the report prepared pursuant to art. 17 of the law of 24 November 1981 n. 689 from the aforementioned Unit it does not appear that the Company has made the payment at a reduced rate;

GIVEN the minutes n. 113 of 3 December 2015, which is intended as fully referred to herein, with which Trivenet s.r.l., in the person of the pro-tempore legal representative, was charged with the administrative violation envisaged by art. 162, paragraph 2-bis, of the Code, in relation to art. 123 (regarding the retention times of traffic data for billing purposes), informing you of the right to make a reduced payment pursuant to art. 16 of the law of 24 November 1981 n. 689;

NOTING that the report prepared pursuant to art. 17 of the law of 24 November 1981 n. 689 from the aforementioned Unit it does not appear that the Company has made the payment at a reduced rate;

HAVING SEEN, furthermore, the minutes no. 114 of December 3, 2015, which is intended as fully referred to herein, by which the administrative violation envisaged by art. 162-bis, in relation to art. 132 of the Code (regarding the retention times of traffic data for the purpose of ascertaining and repressing crimes), informing you of the right to make a reduced payment pursuant to art. 16 of the law of 24 November 1981 n. 689;

NOTING that the report prepared pursuant to art. 17 of the law of 24 November 1981 n. 689 from the aforementioned Unit it does not appear that the Company has made the payment at a reduced rate;

HAVING SEEN, finally, the minutes no. 115 of 3 December 2015, with which the same Company, in the person of the pro-tempore legal representative, was charged with the administrative violation envisaged by art. 162, paragraph 2-bis, in relation to art. 17 of the Code, informing you of the right to make a reduced payment pursuant to art. 16 of the law of 24 November 1981 n. 689;

NOTING that the report prepared pursuant to art. 17 of the law of 24 November 1981 n. 689 from the aforementioned Unit it does not appear that the Company has made the payment at a reduced rate;

GIVEN the defensive writings, dated January 18, 2016, sent pursuant to art. 18 of the law of 24 November 1981 n. 689, with which the party declared that it had "taken all necessary actions to comply and remedy the system criticalities detected during the inspection", with particular reference to the measures necessary to ensure that the data relating to telephone traffic, telematics and data relating to unanswered calls, made from the date of entry into force of the conversion law of decree no. 7/2015, are kept in compliance with the terms of the law. The party noted that, during the internal checks carried out on its systems, "a configuration error was highlighted in the system used with regard to the plaintext requests formulated by its customers. However, the issue identified concerned only a small number of customers with data processed in clear text as a result of legitimately received requests, the data of which, however, were in some cases processed beyond the term of 6 months as required by law ". Faced with this problem, the Company declared that it had ordered the correction of errors on the system and ordered the cancellation of data stored beyond the legal deadlines, in compliance with the provisions of Articles 123 and 132 of the Code. As for the failure of the decryption scripts, detected during the inspections on the server responsible for storing traffic data processed for legal purposes, the Company found that this problem "may be due to an incompatibility of the decryption system with respect to the general one of protection and computerized processing of data, placed hierarchically in a privileged and preordained position within the framework of the protection of the risks referred to in art. 31 of the Code "and in any case to have prepared, even in this case, the corrective measures required by the law . Finally, the party highlighted its economic conditions by requesting that any sanctions imposed be applied in installments, pursuant to art. 26 of the law n. 689/1981;

READ the minutes of the hearing, held on 2 May 2016, pursuant to art. 18 of the law n. 689/1981, with which the party

reserved the right to produce further documentation regarding the findings raised with the notification reports;

GIVEN the additional documentation, sent on May 17, 2016, with which the party declared that:

- with reference to minutes no. 112, the data relating to unanswered calls were kept beyond the term of thirty days "exclusively due to a problem of setting the telephone data management software, which did not allow an automatic split between the tags of the unanswered calls compared to those of the successful calls (...). The Company therefore found itself in the need to keep a mandatory data (successful calls) without being able to simultaneously comply with the obligations to cancel the other data (unanswered calls) ";

- with reference to minutes no. 113, "the retention of the data mentioned [telephone and telematic traffic data for billing purposes] beyond the term depended exclusively on the difficulty of the software in use which did not allow the management of the deletion of data from the billing system without even operating the cancellation of the same data, stored on the separate system for legal purposes ". In any case, the party stressed that the problem in question concerned a small number of users and that, in any case, all the deletions of the data stored beyond the terms of the law were carried out;

- with reference to minutes no. 114, "the reasons for the violation found on the Storagebox server are always attributable to the type of software applied and then modified with effect from April 2015";

- finally, with reference to minutes no. 115, "an access system with badge and personal entry code is in use at the selected access area, assigned to each person authorized to enter, which provides for the sending of an e-mail notification of each access to the technical staff in charge of controlling the data center. The system implemented (...) however does not currently envisage a model compatible with biometric access systems. Therefore, even before the verification of the Guardia di Finanza, the Company was already evaluating the most appropriate investment to implement a biometric system that could replace the current access system, thus planning a significant economic investment ". Furthermore, with regard to the failure to adopt the strong authentication procedure with respect to the conservation of traffic data for justice purposes, the party noted that the Radius server, in reality, only processes telematic data for the purposes of ordinary billing management and, therefore , the use of biometric access systems or cryptographic techniques is not required;

- in conclusion, the party noted that "the criticalities found were determined by the use of a software for the management system of telephone and telematic data with an update defect, not compatible with the changes imposed on the processing of data by the anti-terrorism decree of 2015 . This defect entailed for the Company a violation of different administrative

provisions (heterogeneous formal competition), but nevertheless attributable to the two essential cases of non-deletion of data and the implementation of biometric recognition obligations, where applicable. (...) This is therefore the case. of shortcomings due to objective causes not attributable to the company, but deriving from management software in circulation unsuitable for modification ";

CONSIDERING that the arguments put forward are not suitable to exclude the responsibility of the party in relation to what is disputed. In fact, the party charged the non-compliance with the provisions on data retention mainly to a problem of setting up the systems used for the storage of traffic data, which would have prevented the separation of telephone traffic data from those relating to calls without response (with the consequent conservation of the latter beyond the legal deadline), as well as the cancellation within the legal deadline of the data processed for billing purposes (without also deleting the data processed for other purposes, stored on the same system). In reality, the software configuration and / or setup error cannot be qualified as an "objective cause not attributable to the company", that is, such as to exclude the liability of the Company with respect to the offenses found. It has been repeatedly stated in jurisprudence (and reaffirmed by the Guarantor in its provisions) that the error on the lawfulness of the conduct (referred to as "good faith"), can be relevant in terms of exclusion of liability only when it is inevitable and innocent: it is necessary , therefore, a positive element, foreign to the perpetrator of the violation, such as to generate the conviction of the lawfulness of his action, in addition to the condition that the author has done everything possible to observe the law and that no reproach can be moved to him (Cass. Civ. Section work. July 12, 2010 n. 16320). In addition to the consideration that these requirements are not found in the case that concerns us (given that all the problems identified were easily verifiable with the ordinary diligence required), the position of the Company must also be considered, professionally inserted in a specific field of activity, and , as such, bound to a more specific information and knowledge obligation regarding the rules governing their sector of activity. Among other things, if the party had carried out the internal audit procedures required by the provision on data retention, it would certainly have verified the existence of these problems even before the inspection and remedied. These observations also apply to the arguments put forward with regard to the strong authentication procedures that have not been implemented, since, even in this case, having verified the incompatibility of its system with the requirements set out in the provision of the Guarantor, the party could have remedy it even before the inspection. On the other hand, as regards the argument put forward by the party, according to which the violations found are attributable to the two cases of failure to delete data within the terms of the law and to the failure to implement strong

authentication measures, the inapplicability of the case in question is noted. Institute of the "heterogeneous formal competition" pursuant to art. 8, paragraph 1, of law no. 689/1981. In fact, the application prerequisite of the formal competition is the uniqueness of the action or omission, while, in the case in question, the disputed cases are substantiated by different and unrelated conducts.

Finally, with regard to the observations made, it is noted that, in the assessment report of 21 October 2015, it appears that the traffic data processed for billing purposes are stored on the server called BDC, while the traffic data processed for purposes of assessment and repression of crimes on the server called Radius, which "copies its entire content inside the StorageBox server", as the party itself confirmed in the supplementary documentation sent on November 6. The provision adopted by the Guarantor on January 17, 2008 requires that specific IT authentication systems be adopted, based on strong authentication techniques, to access traffic data, processed for both billing and justice purposes. Furthermore, for the latter, one of the technologies is required to be based on the biometric processing of the person in charge, whose presence was found only for access to the StorageBox server. Therefore, what has been verified and has become an important object is the absence of the strong authentication technique for accessing the "Details" and "Central" folders on the BDC server (see minutes of 21 October 2015, pp. 4 and 5), required for the storage of data processed for billing purposes and the lack of the biometric procedure (as well as cryptographic techniques) for access to the Radius server, for the purposes of protecting data processed for legal purposes (see minutes of the 22 October, p. 3);

NOTING, therefore, that Trivenet s.r.l., on the basis of the aforementioned considerations, as data controller, pursuant to art. 4 and 28 of the Code, it appears to have carried out a processing of traffic data:

a) in violation of art. 162-bis, of the Code, in relation to art. 132, paragraph 1-bis, for having kept the data relating to unanswered calls for a period exceeding thirty days;

b) in violation of art. 162, paragraph 2-bis, of the Code, in relation to art. 123, paragraph 2, for having kept the telephone traffic data for billing purposes for a period exceeding six months;

c) in violation of art. 162-bis of the Code, in relation to art. 132, paragraph 1 of the Code, for having kept the telephone and telematic traffic data for the purpose of ascertaining and suppressing crimes for periods of more than 24 months and 12 months respectively;

d) in violation of art. 162, paragraph 2-bis of the Code, in relation to art. 17, pursuant to art. 167 of the Code, for having carried

out a processing of telephone and electronic traffic data for the purpose of ascertaining and repressing crimes without adopting the measures prescribed by the Guarantor with the provision of January 17, 2008, amended and integrated by the subsequent provision of July 24, 2008 in subject of conservation of telephone and telematic traffic data;

GIVEN art. 162-bis, of the Code which punishes the violation of the provisions indicated in art. 132, paragraph 1, of the Code with the administrative sanction of the payment of a sum from ten thousand euros to fifty thousand euros;

GIVEN art. 162, paragraph 2-bis, of the Code which punishes the violation of the provisions of art. 167 of the Code which refers, among others, to articles. 17 and 123, with the administrative sanction of the payment of a sum from ten thousand euros to one hundred twenty thousand euros;

CONSIDERING that, for the purposes of determining the amount of the pecuniary sanction, it is necessary to take into account, pursuant to art. 11 of the law n. 689/1981, of the work carried out by the agent to eliminate or mitigate the consequences of the violation, the seriousness of the violation, the personality and economic conditions of the offender;

TAKING NOTE of the request for payment in installments of the sanctions imposed, formulated by the party in the defense writings on the basis of art. 26 of the law n. 689/1981;

CONSIDERING, therefore, to have to determine, pursuant to art. 11 of the law n. 689/1981, the amount of the pecuniary sanction, based on the aforementioned elements assessed as a whole, to the extent of:

- € 10,000.00 (ten thousand) for the violations pursuant to art. 162-bis of the Code, in relation to art. 132, paragraph 1-bis, of the Code;
- € 10,000.00 (ten thousand) for the violations pursuant to art. 162, paragraph 2-bis, in relation to art. 123, paragraph 2, of the Code;
- € 10,000.00 (ten thousand) for the violations pursuant to art. 162-bis of the Code, in relation to art. 132, paragraph 1, of the Code;
- € 10,000.00 (ten thousand) for the violations pursuant to art. 162, paragraph 2-bis, in relation to art. 17 of the Code;

HAVING REGARD to the documentation on file;

GIVEN the law of 24 November 1981 n. 689, and subsequent amendments and additions;

GIVEN the observations of the Office, formulated by the Secretary General pursuant to art. 15 of the regulation of the Guarantor n. 1/2000;

Rapporteur Dr. Giovanna Bianchi Clerici;

ORDER

a Trivenet s.r.l., with headquarters in Galleria Veneta (PD), Viale Europa n. 20, P.I. 03350610287, in the person of the pro-tempore legal representative, to pay the sum of € 40,000.00 (forty thousand) as a pecuniary administrative sanction, for the violations indicated in the motivation, dividing it, in acceptance of the installment request, in 20 monthly installments of the amount of € 2,000.00 (two thousand) each;

INJUNCES

to the same subject to pay the sum of 40,000.00 (forty thousand) 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 of 24 November 1981, n. 689.

Pursuant to art. 152 of the Code and 10 of the d. lg. n. 150/2011, against this provision, opposition may be proposed to the ordinary judicial authority, with an appeal filed with the ordinary court of the place where the data controller resides, within thirty days from the date of communication of the provision itself. , or sixty days if the applicant resides abroad.

Rome, 25 January 2018

PRESIDENT

Soro

THE RAPPORTEUR

Bianchi Clerici

THE SECRETARY GENERAL

Busia