DECREE NO. 8771, MAY 11 2016

Regulates Law No. 12965, of April 23, 2014, to indicate the admitted cases of discrimination of data packets on the internet and traffic degradation; indicate procedures for the storage and protection of data by connection and applications providers; establish transparency measures for the request of registration data by the public administration and establish parameters to verificate regulatory infringements.

The President of the REPUBLIC, in the use of the attributions given by art. 84, heading, paragraph IV, of the Constitution, and in view of the provisions of law No. 12965, of 23 April 2014,

DECREES:

CHAPTER I

GENERAL PROVISIONS

Art. 1. This Decree deals with the admitted hypothesis for the discrimination of data packets on the internet and traffic degradation; indicates procedures for data protection and storage by connection and applications providers; creates transparency measures for the request of registration data by the public administration and establishes parameters festablish parameters to verificate regulatory infringements.

Art. 2. The provisions of this Decree are applicable to those responsible for the transmission, switching or routing and to connection and internet applications providers; as defined in terms of item I of the heading of art. 5 of law No. 12965, 2014.

Sole paragraph. The provisions of this Decree shall not apply to:

I – telecommunications services not intended for the provision of internet connection; and

II – specialized services; understood to mean services optimized for assured quality of service, security or speed; even if they use TCP/IP or equivalent protocols, provided that:

a) they don't constitute a substitute to the internet in its public and unrestricted character ; and

(b) they are intended for specific groups of users with strict admission control.

CHAPTER II

ON NET NEUTRALITY

Art. 3. The requirement of isonomic treatment contained in art. 9 of law No. 12965, 2014, must ensure the preservation of the public and unrestricted character of internet access and the foundations, principles and objectives of the use of the internet in the country, as provided for in law No. 12965, 2014.

Art. 4. The discrimination or degradation of traffic is an exceptional measure, and it can only arise from technical requirements that are deemed essential for the adequate provision of services and applications or the prioritization of emergency services, as long as all the requirements laid out in art. 9, paragraph 2, of law No. 12965, 2014 are fulfilled.

Art. 5. The technical requirements necessary for the proper provision of services and applications must be observed by those in in charge of the transmission, switching or routing activities, within the range of their own networks. Those requirements shall only be intended to maintain network stability, security, integrity and functionality.

§ 1 The essential technical requirements referred to in the previous paragraph are those arising from:

I – handling of network security issues, such as the restriction on bulk messaging (spam) and denial of service attacks; and

II – administer exceptional situations of network congestion, such as alternative routing in cases of interruption of the main route and emergency situations.

(2) the national agency of telecommunications – (Anatel) will monitor and verify infractions to the technical requirements listed in this article, considered the guidelines established by the Steering Committee of the Internet – (CGI.br).

Art. 6. In order to achieve the proper provision of services and applications on the internet, network management allowed in order to preserve network stability, security and functionality; only by using technical measures that are compatible with international

standards and developed for the adequate operation of the internet. The regulatory parameters issued by Anatel shall be observed and the guidelines established by the CGI.br are to be considered.

Art. 7. Those responsible for the transmission, switching or routing must adopt transparency measures to clarify to the the user the reasons for network management involving discrimination or degradation as stated in art. 4, such as:

I- a reference in the service contracts signed with end users or application providers; and

II- the publishing of information regarding adopted management practices in their web sites, through easy-to-understand language.

Sole paragraph. The information mentioned in the past article should contain, at least:

I – the description of those practices;

II- the effects of their adoption in the quality of user experience; and

III – the reasons and the need for the adoption of those practices.

Art. 8. The degradation or discrimination resulting from the prioritization of emergency services may only arise from:

I-communications directed to emergency service providers, or communications among them, as provided for in the regulations of the national agency of telecommunications – Anatel; or

II-communications that are necessary to inform the population in situations of risk of disaster, emergency or state of public calamity.

Sole paragraph. The data transmission in the cases listed in this article will be free.

Art. 9. The following unilateral practices and agreements between those responsible for transmitting, switching or routing and application providers are forbidden:

I – those that compromise the public and unrestricted character of internet access and the fundamentals, principles and goals of internet usage in the country;

II-prioritize data packages due to commercial arrangements; or

III-favor applications offered by those responsible for transmitting, switching or routing or by companies in the same economic group.

Art. 10. Commercial offerings and billing models for internet access must preserve a single internet that is open, plural and diverse in nature and understood as a means for the promotion of human, economic, social and cultural development as well as contributing to the building of an inclusive and non-discriminatory society.

CHAPTER III

ON THE PROTECTION OF RECORDS, PERSONAL DATA AND PRIVATE COMMUNICATIONS

Section I

On the request of registration data

Art. 11. The administrative authorities referred to in art. 10, paragraph 3, of law No. 12965, 2014, shall indicate the legal grounds for their access powers and the motivation for their requests of access to registration data.

§ 1 The provider that does not collect registration data should report that fact to the requesting authority, thus getting exempt from providing such information.

§ 2 Registration data consists on:

I – filiation information;

II – address; and

III – personal information, understood as name, surname, marital status and occupation of the user.

§ 3 the aforementioned requests must specifically indicate the individuals whose data are being requested and the desired information. Bulk requests, that are generic or nonspecific are not allowed.

Art. 12. The highest authorities of each organ of the federal public administration shall publish yearly statistical reports on registration data requests on their websites. Those reports must contain:

I – the number of requests made;

II - a list of the connection or application providers targeted by data requests;

III – the number of requests granted and refused by the connection and access to applications providers; and

IV – the number of users affected by such requests.

Section II

Standards for the security and confidentiality of records, personal data and private communications

Art. 13. Connection and application providers must observe the following guidelines on security standards in the custody, storage and processing of personal data and private communications:

I – the establishment of strict controls over access to data; by instituting responsibilities for those who have access and exclusive access privileges for certain users;

II - the provision of authentication mechanisms for access to records, by using, for example, dual authentication systems to ensure the individualization of those responsible for data processing;

III – the creation of detailed access logs to connection and applications records. Those records shall contain the time and duration of access, the identity of the official or company appointed administrator involved and the identification the files accessed. These safeguards apply even in the case of compliance with the provisions of art. 11, paragraph 3, of law No. 12965, 2014; and

IV – the use of records management solutions through techniques that guarantee the inviolability of the data, such as encryption or equivalent protection measures.

§1 It is the responsibility of the CGIbr to promote studies and recommend procedures, as well as technical and operational standards for the provisions of this article, in

accordance with the specificities and the size of the connection and application providers.

§2 In view of the provisions of sections VII to X of the heading of the art. 7 of law No. 12965, 2014, connection and applications providers must retain as little personal data, private communications and connection and access to applications records as possible. That information shall be deleted:

I – after the purpose of their use is achieved; or

II – after the deadline determined by the legal obligation is due.

Art. 14. For the purposes of the provisions of this Decree, the following definitions are provided:

I – personal information (or personal data) – data related to an identified or identifiable natural person, including identifying numbers, location data or electronic identifiers, when these are related to a person; and

II-processing of personal data – any operation carried out with personal data, such as: collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, disposal, evaluation or control of information, communication, modification, transfer, dissemination or extraction.

Art. 15. The data referred to in art. 11 of law No. 12965, 2014, should be kept in an interoperable and structured format, for easy access in case of court decision or legal determination, while respecting the guidelines listed in art. 13 of this Decree.

Art. 16. The information about the security standards adopted by application and connection providers should be disclosed in a clear and accessible way to any interested party, preferably through their web sites, while respecting the right of confidentiality with regard to business secrets.

CHAPTER IV

ON SUPERVISION AND TRANSPARENCY

Art. 17. The Anatel will act in the regulation, monitoring and verification of infractions under Law n 9,472, from July 16, 1997.

Art. 18. The National Secretariat of the consumer will act on the monitoring and verification of infractions, pursuant to law n 8078 of September 11, 1990.

Art. 19. The calculation of economic violations shall be in charge of the Brazilian competition Defense System,pursuant to law no 12529, of 30 November 2011.

Art. 20. The organisms and entities of the federal public administration with specific competence regarding issues related to this Decree will act collaboratively, considered the CGIbr guidelines, and must ensure compliance with brazilian legislation, including the application of sanctions, even if the activities are carried out by legal person based abroad, pursuant to art. 11 of law No. 12965, 2014.

Art. 21. The verification of infractions of the law n 12965, 2014 and this Decree will follow the internal procedures of each of the controlling entities and may be initiated ex officio or upon request of any interested party.

Art. 22. This Decree shall enter into force thirty days after the date of its publication.

Brasília, May 11, 2016; 195th and 128th of the Republic's independence.

DILMA ROUSSEFF

Eugênio José Guilherme de Aragão

André Peixoto Figueiredo Lima

João Luiz Silva Ferreira

Emília Maria Silva Ribeiro Curi

Translation: Javier Pallero (Access Now) javier@accessnow.org