Revista DIREITO GV

ISSN 2317-6172

v. 19 | 2023

PUBLICAÇÃO DA

ESCOLA DE DIREITO DE SÃO PAULO
DA FUNDAÇÃO GETULIO VARGAS

FGV DIREITO SP

V. 19
2023
ISSN 2317-6172

Revista DIREITO GV

FGV DIREITO SP

Recebido: 28.09.2021
Aprovado: 09.03.2023

https://doi.org/10.1590/2317-6172202335

Personal Data of Adolescents in Higher Education: The LGPD and the Use of Digital Media for Teaching Activities and Remote Testing[1]

DADOS PESSOAIS DE ADOLESCENTES NA EDUCAÇÃO SUPERIOR: LGPD E UTILIZAÇÃO DE MEIOS DIGITAIS PARA ATIVIDADES DE ENSINO E APLICAÇÃO DE PROVAS

Thaís Duarte Zappelini[1], *Laurianne-Marie Schippers*[2] e *Alexandre Pacheco da Silva*[3]

Abstract
With the spread of the new Coronavirus, Higher Education Institutions (HEIs) needed to adapt to this reality. The implementation of Emergency Remote Teaching (ERT) in Brazil relied on the experiences of distance education (EaD). Also, there was a significant increase in the use of remote testing tools that rely on monitoring (e-proctoring). This context has generated several concerns regarding the protection of vulnerable data subjects. The main objective of this article is to assess the processing of adolescents' personal data by HEIs in the context of teaching activities carried out by digital means and the use of remote testing that include the collection of sensitive data. For this purpose, we aim to analyze the protective regime for children and adolescents' sensitive information in Brazil's General Personal Data Protection Law (LGPD), the appropriate legal bases for their management, and the best practices to be adopted. As a result, we have concluded that specific consent is not the only legal basis applicable to processing data from minors. However, it represents an important possibility of data management by legal guardians and the protection of underage people. In any case, the principles of necessity and transparency must be part of this choice process.

Keywords
LGPD; adolescents; distance education; emergency remote learning; remote testing.

Resumo
Com o alastramento do novo Coronavírus, as Instituições de Ensino Superior (IES) precisaram adaptar-se a essa realidade. O implemento do Ensino Remoto Emergencial (ERE) no Brasil contou com o aproveitamento de experiências da Educação a Distância (EaD). Além disso, houve significativo aumento no uso de ferramentas de aplicação de provas remotas que contam com monitoramento (e-proctoring). Esse contexto gerou diversas preocupações quanto à proteção de dados pessoais no ensino, especialmente de titulares vulneráveis. O presente artigo tem como principal objetivo apreciar o tratamento de dados pessoais de adolescentes pelas IES no âmbito de atividades de ensino realizadas por meios digitais e aplicação de provas remotas que contem com a coleta de dados sensíveis. Para tanto, são analisados o

1 Lemann Center for Brazilian Studies, University of Illinois at Urbana-Champaign, Champaign, Illinois, United States of America
https://orcid.org/0000-0001-7765-4502

2 Centro de Ensino e Pesquisa em Inovação, Escola de Direito de São Paulo da Fundação Getulio Vargas, São Paulo, São Paulo, Brazil
https://orcid.org/0009-0002-6508-958X

3 Centro de Ensino e Pesquisa em Inovação, Escola de Direito de São Paulo da Fundação Getulio Vargas, São Paulo, São Paulo, Brazil
https://orcid.org/0000-0002-1028-9392

1 This paper was developed at the Center for Education and Research on Innovation (CEPI – FGV DIREITO SP), by its coordinator and researchers, in the Law, Technology and Society research fields.

regime protetivo para dados de crianças e adolescentes na Lei Geral de Proteção de Dados Pessoais (LGPD), as bases legais adequadas para o seu tratamento e as melhores práticas a serem adotadas. Como resultados da análise, concluiu-se que o consentimento específico não é única base legal aplicável a operações realizadas com dados de menores. Porém, representa importante possibilidade de gestão pelos responsáveis e proteção do menor. Em qualquer caso, os princípios da necessidade e da transparência devem integrar esse processo de escolha.

Palavras-chave
LGPD; adolescentes; educação a distância; ensino remoto emergencial; provas remotas.

Introduction

The Brazilian General Personal Data Protection Law (Law No. 13.709/2018 – hereinafter "LGPD") is a transversal rule that permeates the activities of various economic sectors in Brazil. In this regard, the routine of Higher Education Institutions (HEIs) encompasses a series of operations carried out with an expressive volume of data from students, employees, and third parties. In March 2020, with the state decree of public calamity in Brazil[2] and the replacement of in-person classes with lessons conducted using digital media,[3] HEIs were obliged to implement emergency measures to continue the school year.

With the COVID-19 pandemic, the need to quickly adapt to this context made many HEIs take advantage of the experience of distance education (EaD), a teaching modality that has been used in the country since the beginning of the 20th century. Thus, we sought to establish the Emergency Remote Teaching (ERT), similar in many aspects to EaD, also regarding specific concerns with the protection of the personal data of students and teachers. As it will be described below, the ERT also features its own characteristics, starting with its legal framework and regulatory requirements.

2 Reference to Legislative Decree No. 6, of March 20th, 2020 (BRASIL, 2020a).

3 In March 2020, the Emergency Operating Committee of the Ministry of Education (COE-MEC) was established and determined the replacement of in-person learning for classes conducted in digital media, under Ordinance No. 343/2020 and Provisional Measure No. 934 /2020, while the New Coronavirus pandemic situation lasted.

It is common for children under 18 years of age to be enrolled in undergraduate courses,[4] and, more than that, in selective processes such as the college entrance examination, which manages varied personal information from young people below this age group. In addition, this type of exam has also undergone important transformations with the use of tools for remote testing, which may depend on the collection of biometric data (sensitive personal data in the context of the LGPD) and on monitoring the candidate during the exam.

Therefore, the main objective of this study is to approach the problem of processing adolescents' personal data, considering the use of digital tools for teaching activities and the use of remote testing in the context of HEIs. It starts with three essential developments in the scenario presented in the LGPD's protection regime: (i) teaching activities within the scope of EaD and ERT; (ii) recording of lessons; and (iii) remote examinations that involve the collection of sensitive data.

We propose an analysis of the personal data protection legislation, indicating the legal bases that justify the processing operations performed, the necessary measures to comply with the principles of personal data protection, and the appropriate means to fulfill the rights of data subjects. This is an exploratory study, as there is little literature in Brazil on the debate, and it is still an incipient field due to the contemporaneity of the implementation processes of these teaching technologies in the pandemic context, as well as regarding the discussion on the data protection from underage data subjects in this background.

In addition to that, there is the fact that Art. 14, § 1, of the LGPD stipulates that "the processing of children's personal data must be carried out with the specific and prominent consent given by at least one of the parents or by the legal guardian". The omission of adolescents in § 1 raises an interpretative question: it is not clear whether the need to obtain the consent of parents or guardians, provided for children, applies extensively to adolescents, or if other legal bases provided for in the list of articles 7 and 11 of the LGPD are also applicable to them.

In line with international treaties and conventions to which Brazil is a signatory,[5] the Brazilian legal system assumes that children and adolescents are vulnerable people. This is because they are in a physical, mental, moral, spiritual, and social development phase (Art. 3 of the Child and Adolescent Statute – ECA), and they need *full, special, and priority protection*. It means that they may be less aware of the risks, consequences, and guarantees for

4 According to a survey by the Brazilian Association of Internships, 23,343 young people under the age of 18 attend Higher Education in Brazil (ABRES, 2020).

5 Take the example of the Convention on the Rights of the Child (Decree No. 99,710/1990) and the American Convention on Human Rights (Pact of San José, Costa Rica, Legislative Decree No. 27/1992).

their fundamental rights and freedoms regarding the processing of personal data, as they do not have the same insight as adults to understand the implications of the operations to which they are exposed to and how to exercise their rights as data subjects.

The main question raised by this article is: what are the limits of the applicability of Art. 14, § 1, from the LGPD for children and adolescents and what are the consequences of these limits for using digital media for teaching activities and exams in Higher Education? It will be examined by considering the changes caused in the Higher Education in Brazil by the pandemic context.

This topic reflects the importance of discussing how the scope of the LGPD offers data protection for minors, dialoguing with other norms of the Brazilian legal system. Furthermore, it is important to understand which alternatives are available to deal with an unprecedented reality, especially considering that many articles of the law only came into force 24 months after their publication date (Art. 85, II).

To develop this theme, it is assumed that, although the LGPD does not discriminate the data of children and adolescents as sensitive (list of Art. 5, II), this information is part of a special data category, as the law grants it a specific protective regime, imposing stricter obligations on the agents who carry out data processing.

Considering the application problem of Art. 14 of LGPD, which does not clearly present the hypotheses for children and adolescents, an inductive methodology is proposed with a critical analysis of the difficulties of the Brazilian case faced by the recent personal data protection law, particularly in a context that has experienced digitalization of teaching. In a digital environment, vulnerable people, such as children and adolescents who do not have the full discernment to understand all the risks to which they are exposed to need redoubled protection. The LGPD issue also concerns the systematic application of related legislation on children and adolescents.

The bibliographic survey was used as the main research technique. International references were selected for the background of this work, especially the ones related to data protection authorities and materials produced on the General Data Protection Regulation (GDPR) as guidelines, considering that the subject in vogue is recent in Brazil.

We seek to bring interpretations about the scope of Art. 14 and perceptions about what would be the best practices of application in the LGPD for children and adolescents, considering the digitalization of education. This proposition also emerged from the joint professional experience of the authors after two years dedicated to studying compliance strategies for the LGPD in Brazil, which resulted in the elaboration of materials and guidelines for the adequacy of procedures aimed at Higher Education, especially considering how Brazilian legislation differentiates the capacity of agents in civil law while providing integral and special protection for children and adolescents.

The intersection between these norms reveals the need for a harmonic interpretation of Brazilian laws. The major question is how to guarantee the protection of these vulnerable

people without taking away their autonomy and providing them enough information in addition to ensuring that those responsible for them have a full understanding of their rights.

The first part of this paper introduces the discussion on the LGPD's protection regime for data on children and adolescents and the legal basis applicable to its processing, pointing out that, based on a systematic interpretation of Brazilian legislation, adolescents between 12 and 16 years of age should be prioritized under the rule provided in Art. 14, § 1st, of the LGPD, requiring specific and prominent consent from at least one parent or guardian. It should be noted, however, that this is not the only applicable legal basis.

Next, EaD is differentiated from ERT based on its legal frameworks through the analysis of the applicable legal basis in each of these segments, in order to carry out teaching activities (synchronous and asynchronous). The modalities are considered in parallel, in view of their approximations in the use of digital media as tools for teaching, especially regarding virtual environments and videoconference platforms, which involve the collection, storage, and use of students' personal information.

The third part deals with the processing of sensitive personal data of children and adolescents. The processing of some kinds of information can create significant risks for the fundamental rights of vulnerable people, by itself or from inferences. It is appreciated, in this context, the issue of recording classes and using remote tests with the assistance of tools that rely on the collection of sensitive data, such as biometric data, and monitoring the candidate during the test.

1. The Data Protection Regime for Children and Adolescents

To understand which legal bases are more suitable for the processing of minors data, the first step is to reflect on the protection regime granted to them by the LGPD, presented in Section III, Chapter II, and within the provisions "The Processing of Personal Data of Children and Adolescents".

The referred chapter is exclusively composed of Art. 14 and its six paragraphs, which establish that the processing of personal data of children and adolescents must be carried out in their best interest. Art. 14, § 1, of the LGPD stipulates that "the processing of personal data of children must be carried out with the specific and prominent consent given by at least one of the parents or by the legal guardian". The letter of the law refers to information about children without expressly alluding to how the personal information of adolescents should be processed. There is also no definition, in the LGPD, about who is the child or the adolescent. In other words, there is no mention of the average age of both groups or their civil capacity.

This legal basis presents a difficulty in the fact that the controller must make all reasonable efforts to verify whether the consent was effectively given by the person responsible for the child or adolescent, considering the available technologies (Art. 14, § 5, of the

LGPD).[6] That is one of the challenges for collecting personal data from children (CCGD, 2020, p. 30). Furthermore, it is the legal obligation of the controller to publicly keep the information on the types of data collected, their use, and the procedures for exercising the rights of data subjects (Art. 14, § 2).

The LGPD offers possibilities of waiver of consent. In this way, exceptionally, it is possible to collect personal data from children without the consent of parents or guardians, and contact them only when necessary or for the children's protection. In this case, data must be used only once and should not be stored, and under no circumstances may it be shared with third parties without due consent (Art. 14, § 3, LGPD).

In this sense, Article 14, § 4, of the LGPD provides that the data controller cannot condition the participation of the data subjects referred to in § 1 in games, internet applications, or other activities to the provision of personal information, unless they are strictly necessary for the activity. Moreover, it is worth highlighting the duty of transparency brought by § 6 of the same article, which requires that information on processing minor's data must be provided in a simple, clear, and accessible way, considering the characteristics of the user, with the assistance of audiovisual resources when appropriate, providing the necessary information to parents or guardians and adequate information for the child's understanding.

Given what the LGPD postulates regarding operations carried out with data from minors, it is necessary to limit the data subjects to which Art. 14, § 1, refers. Although the law does not mention age brackets, the Child and Adolescent Statute (ECA)[7] certainly provides that a child is a person who is not fully 12 years old, while the age bracket for an adolescent ranges between 12 to not fully 18 years old (Article 2nd).[8] Thus, if individuals are 11 years, 11 months and 28 days old, for example, they will still be considered as children until they are effectively 12 years old. Likewise, adolescents who seek to carry out an act of civil life that is

6 The authority of the United Kingdom (ICO – Information Commissioner's Office), in its Guide on the General Data Protection Regulation (GDPR), presents an interesting position on what these "reasonable efforts" would be (ICO, 2018).

7 Art. 14 of the LGPD establishes, in its *caput*, that the processing of personal data of children and adolescents must be carried out in their best interest. We see that the provision is consistent with the ECA, in providing for this general principle – which expresses the full protection of children and adolescents – and with 227, *caput*, of the Federal Constitution of 1988, which establishes the duty of the family, society, and State to ensure children, adolescents, and young people, with "absolute priority", the rights to life, health, food, education, leisure, professional training, culture, dignity, respect, freedom and family and community coexistence, safe from all forms of negligence, discrimination, exploitation, violence, cruelty, and oppression.

8 In exceptional cases, ECA can be applicable to people up to 21 years old, as in Art. 121, § 5.

only allowed for people aged of 18 years old will not be able to do so, even if there are only a few days left to reach that age. Practical consequences of this differentiation can be seen in the capacity regime of the Civil Code (CC) of 2002 (BRASIL, 2002), which evidences that minors under 16 years of age are absolutely incapable of personally performing acts of civil life (Art. 3, CC) and that those over 16 and under 18 are relatively incapable of certain acts of civil life or understanding how they are exercised (Art. 4, I, CC). In this regard, it should be noted that the Code establishes that (i) legal transactions joined by absolutely incapable persons – which cover minors under 16 years of age – are null (Art. 166, CC), and that (ii) those joined by relatively incapable persons are voidable (Art. 171, CC), and may be confirmed by the parties, except for the rights of a third party (Art. 172, CC).

At this point, there is an essential difference: children under 16 years old must be represented by their parents or guardians, and those over 16 should be assisted. In a simple language, it is possible to state that, in the first hypothesis, those responsible make decisions and carry out the management of the minor's civil life and, in the second case, "monitor" young people, ensuring the regularity of their actions. 16-year-old adolescents can, for example, vote, travel unaccompained to a region outside from where they live (Art. 83, CC), and emancipate themselves (Art. 5, sole paragraph, CC), among other acts. It leads us to the conclusion that Brazilian law considers that, although minors under 16 years of age cannot independently perform all acts of civil life without being assisted, they are more discerning than young people below that age, as they already are in a condition of physical, mental, moral, spiritual, and social development (Art. 3, ECA) closer to adulthood, which is, 18 years old according to Brazilian law.

It is possible, therefore, to proceed with a logical-systematic interpretation of the indicated norms, observing the best interest of the minors brought by the ECA (BRASIL, 1990), as well as for the full (Art. 1, ECA) priority (Art. 4, ECA) and special protection of children and adolescents and considering the limitations for each age group indicated in the Statute and in the Civil Code.

In other words, it is not postulated that consent is the exclusive basis for the processing of data from children and adolescents, but Art. 14, *caput*, brings the notion that parents need to have a certain control to manage the data in the best interest of the minor. Art. 14, § 1, provides a special consent, as the most used basis also for adolescents, valuing their protection. Consent represents an important tool for parents to be able to protect the rights of children and adolescents.

Evidently, given the discipline of capacity of the Civil Code and respecting the freedom and autonomy of young people, the 16-year-old adolescent has a greater range of management over certain acts of civil life or the way to exercise them.[9] The table below summarizes

9 It is worth mentioning that, in the GDPR (General Data Protection Regulation – Regulation EU, 2016/679), 679/2016, the rule is that consent must be given by those responsible for persons under 16

the analysis carried out during the study, for a better understanding of the age group criteria and the interaction between the provisions of the standards considered herein.

TABLE 1 – **DIFFERENTIATION OF CHILDREN AND ADOLESCENTS ACCORDING TO THE CRITERION OF AGE AND RELATIONSHIP BETWEEN THE PROVISIONS OF THE ECA, CC, AND LGPD**

	CHILD	**ADOLESCENT**
ECA (CHILD AND ADOLESCENT STATUTE)	A PERSON **WHO IS NOT FULLY 12 YEARS OLD** (ART. 2, ECA).	A PERSON WHO IS BETWEEN **12 AND NOT FULLY 18 YEARS OLD** (ART. 2, ECA).
CC (CIVIL CODE)	**ABSOLUTELY INCAPABLE** OF PERSONALLY EXERCISING THE ACTS OF CIVIL LIFE (ART. 3, CC), AND MUST BE REPRESENTED BY THEIR PARENTS/LEGAL GUARDIANS.	**RELATIVELY INCAPABLE** OF CERTAIN ACTS OF CIVIL LIFE OR HOW TO EXERCISE THEM (ART. 4, I, CC).
LGPD	**RULE** (ART. 14, § 1): THE PROCESSING OF PERSONAL DATA **OF CHILDREN** MUST BE CARRIED OUT WITH THE SPECIFIC AND PROMINENT CONSENT GIVEN BY AT LEAST ONE OF THE PARENTS OR BY THE LEGAL GUARDIAN. **EXCEPTIONS TO THE LAW (WAIVER OF CONSENT):** TO CONTACT THE PARENTS OR LEGAL REPRESENTATIVES OR FOR THEIR PROTECTION.	ALTHOUGH SECTION III OF CHAPTER II OF THE LAW RELATES THE "PROCESSING PERSONAL DATA OF CHILDREN AND **ADOLESCENTS**", IT DOES NOT INCLUDE THE LATTER IN THE RULE OF ART. 14,§ 1. CONSIDERING THE BEST INTEREST AND THE COMPREHENSIVE, SPECIAL, AND PRIORITY PROTECTION REGIME FOR CHILDREN AND ADOLESCENTS IN THE BRAZILIAN LEGAL SYSTEM, **IT IS RECOMMENDED TO USE THIS RULE FOR CHILDREN UNDER 16,** WHO ARE ABSOLUTELY INCAPABLE.

Source: Authors' own elaboration.

years of age. However, the Member States of the European Union may provide this purpose for a lower age, respecting the limit of 13 years old, in order to avoid conflicts with the internal legislation of the Member States. That is, the Member States can define that, from the age of 13, adolescents offer their consent without the need for support from their parents or guardians. In this regard, the Guide on the GDPR and the rights of children and adolescents of the European Data Protection Board (EDPB) states that consent is, in many cases, the preferred basis for legitimizing data processing activities, so that the Art. 8 (1) of the GDPR applies to information society services (i.e.: almost all online services) directly offered to children (EDPB, 2017, p. 12).

Next, we will address the applicable legal bases and requirements for data processing from adolescents in the context of non-face-to-face teaching activities, that is, with the use of digital media.

2. Personal Data of Minors: Emergency Remote Teaching and Distance Education

2.1. Brief History of EaD and ERT in Brazil

In the context of the new Coronavirus pandemic, activities of different levels and modalities were suspended both in Basic and Higher Education, affecting public and private institutions (CASTIONI *et al.*, 2021, p. 2).

Many learning strategies were put into practice in the molds already used in EaD. Before the pandemic, in-person undergraduate courses could already be composed of activities developed in EaD, provided that the maximum workload limit for activities in this modality did not exceed a total of 40%, in compliance with the curricular guidelines of each course (MEC Ordinance No. 2.117, of December 6th, 2019).

Opinion No 5/2020, of the National Council of Education (CNE), provided guidelines to reorganize school calendars (from early childhood to higher education) and to carry out non-face-to-face pedagogical activities during the pandemic period. The text emphasized that remote activities for higher education could be considered for compliance with the minimum annual workload so that it would not be necessary to make up for it after the pandemic (GUSSO *et al.*, 2020, p. 4).

Social isolation as a public health policy and the suspension of on-campus classes proposed Emergency Remote Teaching (ERT) as an alternative for HEIs to be able to continue the school year (CASTIONI *et al.*, 2021, p. 6). Like EaD, ERT makes use of digital media for teaching activities, consequently bringing specific issues for data protection, such as the collection of a greater volume of information from students and the use of platforms to carry out synchronous activities – in real time, with student-teacher interaction – and asynchronous – which can be performed at other times.

Although ERT uses the online environment for teaching curricular subjects, it differs from EaD in its characteristics and implications (GUSSO *et al.*, 2020, p. 4-6), starting with its legal frameworks and regulatory requirements to be fulfilled.

In Brazil, distance education as a teaching modality emerged at the beginning of the 20th century, dating back to the registration of vocational courses by correspondence (CASTIONI *et al.*, 2021, p. 7-8), and has been gaining relevant space among HEIs in the last

decades.[10] Its development was accompanied by new perspectives, in terms of social and digital inclusion, enabling mobility, cost, and accessibility barriers to be overcome.

Distance learning is provided for in the National Education Guidelines and Base Law (Law No. 9,394, of December 20th, 1996), in which article 80 is regulated in Decree No. 9,057, of May 25th, 2017. Art. 1 of the aforementioned Decree which determines that, in distance education, didactic-pedagogical mediation in teaching and learning processes occurs with the use of information and communication means and technologies, with qualified personnel, access, monitoring, and compatible assessment and the development of educational activities for students, as well as for education professionals who are in different places and time zones. For its implementation to occur, the HEIs must require specific accreditation and present adequate physical structure and space to develop certain face-to-face activities (assessments, internships, practices, etc.).[11]

ERT came after the state decree of public calamity in Brazil in March 2020. In April of the same year, the Emergency Operating Committee of the Ministry of Education (COE-MEC) was instituted and published Ordinance No 343/2020 and Provisional Measure No 934/2020, which authorized the replacement of in-person learning with classes provided using digital media tools.

The aforementioned Ordinance then admitted, on an exceptional basis, the replacement of on-campus courses in progress by classes that used information and communication means and technologies by HEIs that are part of the federal education system, also establishing that institutions were responsible for defining which subjects could be substituted, as well as for enabling tools to students that would allow them to monitor the content offered and carry out assessments during the authorization period (Art. 1, § 2). The differences between the characteristics of teaching modalities can be seen in the Table 2 below.

10 According to the Brazilian Ministry of Education census, in 2007, distance education represented 7% of enrollments in undergraduate courses. In 2017, it increased by 17.6%, in other words, distance education currently serves more than 1.7 million students, totalizing a 21.2% share of undergraduate students in the country, while face-to-face modality has been facing a drop in the number of enrollments. Census data from 2017 reveals that one in three students graduates in distance learning and that, for ten years, the growth of newcomers in distance education represented 226%, compared to 19% in on-site modality. Available at: http://portal.mec.gov.br/component/tags/tag/32123#:~:text=Em%202017%2C%20o%20aumento-%20foi,queda%20no%20n%C3%BAmero%20de%20matr%C3%ADculas. Visited on: Aug. 10th, 2021.

11 It should also be noted that MEC Ordinance No. 4.059, of December 10th, 2004, started to allow HEIs, according to the pedagogical and curricular organization of their recognized courses, to offer subjects that are part of the curriculum used in their semi-attendance modality, based on Art. 81 of Law No 9.394, from 1996. It provided that the offer did not exceed 20% of the total course load (Art. 2).

TABLE 2 – **MAIN CHARACTERISTICS OF DISTANCE LEARNING AND ERT**

	DEFINITION	LEGAL MILESTONES	CHARACTERISTICS
DISTANCE LEARNING	THE DIDACTIC-PEDAGOGICAL MEDIATION OCCURS WITH THE USE OF INFORMATION AND COMMUNICATION MEANS AND TECHNOLOGIES, ALLOWING EDUCATION PROFESSIONALS TO REACH STUDENTS IN DIFFERENT PLACES AND TIME ZONES.	PROVISION IN LAW NO. 9,394, OF DECEMBER 20TH, 1996. REGULATED BY DECREE NO. 9,057, OF MAY 25TH, 2017.	INTERESTED HEIS NEED, AS A RULE, TO REQUEST SPECIFIC ACCREDITATION FROM THE FEDERAL GOVERNMENT UNION AND MAY OFFER THE COURSE LOAD IN DISTANCE LEARNING MODALITY ACCORDING TO THE PEDAGOGICAL AND CURRICULAR ORGANIZATION OF THEIR ON-SITE UNDERGRADUATE COURSES, UP TO A LIMIT OF 40% OF THE TOTAL COURSE LOAD (ART. 2 OF MEC ORDINANCE NO. 2.117, OF MARCH 6TH, 2019).
ERT	THIS MODALITY IS ADMITTED ON AN EXCEPTIONAL BASIS AND REFERS TO THE REPLACEMENT OF ON-CAMPUS COURSES IN PROGRESS WITH CLASSES THAT USE INFORMATION AND COMMUNICATION MEANS AND TECHNOLOGIES.	ORDINANCE NO. 343/2020 AND PROVISIONAL MEASURE NO. 934/2020.	EXCEPTIONALLY FOR THE LENGTH OF THE AUTHORIZATION PERIOD. HEIS MUST PROVIDE STUDENTS WITH TOOLS THAT ALLOW THEM TO MONITOR THE CONTENT OFFERED AND CARRY OUT ASSESSMENTS (ART. 1, § 2, OF ORDINANCE NO. 343/2020 OF COE-MEC).

Source: Authors' own elaboration.

Based on the table above, the subsequent topics present a specific analysis of the applicable legal bases for teaching activities in each of the modalities to investigate the practical differences between the characteristics of EaD and ERT for such choices.

2.2. PROCESSING OF DATA FROM ADOLESCENTS IN DISTANCE EDUCATION

When it comes to distance learning, there is an expectation of data subjects that the use of "information and communication technologies" makes their activities viable. On the one hand, there are authoritative legal provisions regarding the use of technological means and, on the other hand, the discretion of HEIs for the choice and use of these means, respecting the restrictions provided for by law.

It is possible to consider, herein, the following purposes: (i) enrollment and (ii) registration in internal systems. Enrollment encompasses data such as RG (ID), CPF (Social Security Number), Voter Registration Card, School Transcript, High School Certificate, proof of military enlistment and/or dismissal, and other documents specified by the institution's bylaws (MEC, Frequently Asked Questions about Higher Education). There are normative provisions that determine the requirements to attend higher education, such as Art. 44, II, of Law No. 9,394/1996, which explains that the completion of High School is a condition for enrollment in a HEI. In this regard, it is possible to say that legal terms may require certain data or documents to perform academic routines. The routines that involve the collection, storage, and access to the aforementioned information, when directly resulting from normative provisions and strictly linked to the enrollment action, are related to the basis of compliance with a legal or regulatory obligation. However, by considering other data requested by the institution that is not closely linked to the action of enrollment and that does not have a legal scope for that, it is necessary to analyze its specific purpose.

Registration in internal systems is imperative for the provision of services, such as consulting grades, attendance, access to the library and the release of the student to enter the premises of the HEI, etc. For this processing routine, information such as full name, email (personal or professional), enrollment number, login, and password are collected, stored, generated, and used. It is an operation that not only is present in this teaching modality, without which the execution of services becomes unfeasible, but can also be based on the execution of a contract.

The legal basis of contract performance can be applied for providing educational services. Once the contract is signed, the processing that directly results from it and is essential to the provision of the service can be maintained throughout its execution even in the case of children under 16 years of age. Evidently, it must contain a provision for the processing in the instrument itself, with a prominent disposition regarding the processing that will be carried out. At this point, if a certain tool is essential for the provision of services, its processing will only be justified by the legal basis we have referred to considering that the processed data is not excessive, is in line with the principle of need, as the desired objective could be independently achieved. This legal basis allows data processing to enforce the contract in which the data subject is a party and/or has an interest in the execution – in this case, taking the course.

However, it should be noted that operations linked to it cannot occur in an excessive, disproportionate, or illegitimate way, beyond the specific purposes defined for the data processing and require more than a mere contractual condition. Regarding personal data and processing operations, there should be an assessment of what is considered as essential or not to fulfill the contractual subject matter, so that, if there are less invasive alternatives, processing will not be required.

Another option is the legal basis of special consent. It should be clarified that it implies a free, informed, and unambiguous expression by the data subject or his/her responsible

person in agreement to process his/her personal data for a specific purpose. Consent cannot, therefore, be presumed, and the data subject must be free to consent or not, so there must be the possibility of revoking that choice.[12]

It is recommended that the registration of consent actually occurs and, for children under 16 years of age, the controller must use reasonable efforts to verify it (e.g., validation email, telephone contact, etc.). Thus, it is possible to evidence that, even when obtained by digital means, the record needs to be stored. Therefore, how would it be possible to revoke consent without knowing from which data subject it was obtained?

And why not using the legal basis of legitimate interest to provide services that benefit the data subject (Art. 10, II, of LGPD)?[13] Although, at first, this basis appears to be a reasonable choice, bearing in mind that these operations are necessary for the exercise of the controller's activities and provision of the respective services, it is certainly not the most suitable for adolescents below 16 years of age, considering the general rule of Art. 14, § 1. Furthermore, the alternatives presented above seek to ensure greater protection and autonomy regarding the exercise of the rights of personal data subjects.

This legal basis can only support the processing of personal data for legitimate purposes, considered from concrete situations, which include (but are not limited to) (i) support and promotion of the controller's activities and (ii) protection, in relation to the data subject, of the regular exercise of their rights or services provision that benefit them, respecting their legitimate expectations and fundamental rights and freedoms, under the terms of LGPD (Art 10).

For the LGPD, the use of the legal basis of legitimate interest implies a strictly grounded freedom of the personal data controller, provided that it acts within the legitimate

12 It should be noted that the LGPD (Art. 5, XII) and the GDPR (refer to Recital 32) stipulate that consent must be free, specific, informed, and unambiguous, in a declaration that can be freely withdrawn without negative consequences for the individual.

13 Art. 6, "f", of the GDPR deals with the legality of the processing, including that it is necessary for the legitimate interests of the controller or third parties, except when they are replaced with the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, especially when the data subject is a child. When the case involves the basis of legitimate interest (Art. 7, IX, LGPD) in the data processing on adolescents and children (Art. 6, GDPR), a careful analysis of its use is warranted. The legitimate interest imposes a burden on the personal data controller, that is, the so-called "proportionality test" or "legitimate interest assessment". This burden becomes even more important given the situation of greater vulnerability of children and adolescents who represent data subjects. Furthermore, we note that the GDPR, for example, establishes that this legal basis cannot be adopted in relation to advertising, profiling, targeting and analysis, as well as categorization processes, for processing data from children and adolescents.

expectations of the data subject and respects, above all, the fundamental rights and freedoms of that individual. It is also necessary to note that the data processed under this legal basis must comply with the principles of need and transparency: for each type of processing operation, a proportionality test must be carried out.

2.3. ERT, Pandemic and Operations Carried out with Data from Adolescents

Taking into account the pandemic situation, in which the suspension of in-person classes and the temporary replacement of remote learning was determined, HEIs needed to adapt to the use of digital media, collecting a greater volume of data from students and carrying out their pedagogical projects in a different way than initially intended.

When the enrollment and the execution of the respective contract arose, data subjects and those responsible for them were informed that some operations would be essential for the provision of services, but not necessarily that those means would be used to operationalize asynchronous and synchronous activities. Thus, unlike distance learning, ERT is an exceptional and temporary modality (as long as the authorization period lasts).

ERT was imposed by legal and regulatory requirements. Even so, there was a certain permissibility of choice as to which means could be used by the institutions, provided that this option was able to provide access, availability, and monitoring of the content offered, as well as carrying out evaluations during the period of authorization (Article 1 of MEC Ordinance No. 343, of March 17th, 2020). In other words, the discretion mentioned herein does not refer to whether or not migrate to remote education but it actually resides in the design of the technologies to be employed.

Within the scope of GDPR, regarding the purposes pursued by the Universities with the processing in that period, educational purposes (e.g., Italian Data Protection Authority), public interest or, depending on the jurisdiction, contractual need were alleged. However, operations carried out with secondary purposes, such as promotional ones, would need to be anchored on other bases, such as legitimate interest. In any case, processing can only take place for what it is specified, explicit, and legal according to the purposes for which the data was collected (ANGIOLINI *et al.*, 2020, p. 54).

Many European universities, covered by the scope of GDPR – such as the Universities of Dublin City (DCU, 2020) and Edinburgh (TUE, 2020) – began to use the basis of Article 6, (1) (e), of the aforementioned Regulation during the pandemic period, which stipulates that "processing is necessary for the performance of a task of public interest or in the exercise of the official authority responsible for the processing". This basis was applied due to the extraordinary circumstances of the continuous public health emergency caused by COVID-19, justifying that, similarly to what happened to all HEIs and society in general, HEIs had to quickly adapt to ensure the safety of students and staff, along with the delivery of classes.

From this perspective, we would have as much adequate legal bases as possible for the fulfillment of a legal obligation for people over 16 years of age and, for people under it, the

fulfillment of a legal or regulatory obligation or consent. It is possible, in this context, to evidence a problem in the implementation of special consent considering that, if the guardians of a child or an adolescent did not consent, they would be left with no alternatives to continue the course. Also, there is the issue of operationalizing consent in an emergency situation as the database used to store the record of information on data subjects who consented or not would have to be segmented, and a structure that would enable its revocation would also be necessary. A summary of the item under discussion can be seen in the Table 3.

TABLE 3 – **ROUTINELY RECOMMENDABLE LEGAL BASIS – DISTANCE LEARNING AND ERT**

MODALITY	OPERATION	DATA	LEGAL BASIS	LEGAL BASIS UNDER 16 YEARS OF AGE
DISTANCE LEARNING	ENROLLMENT	RG (ID), CPF (SOCIAL SECURITY NUMBER), VOTER REGISTRATION CARD, SCHOOL TRANSCRIPT, HIGH SCHOOL CERTIFICATE, PROOF OF MILITARY ENLISTMENT AND/OR DISMISSAL.	EXECUTION OF CONTRACT OR PRELIMINARY PROCEDURES AT THE REQUEST OF THE DATA SUBJECT.	SPECIFIC AND HIGHLIGHTED CONSENT, GIVEN BY AT LEAST ONE OF THE PARENTS OR LEGAL GUARDIANS. COMPLIANCE WITH LEGAL OR REGULATORY OBLIGATIONS.
DISTANCE LEARNING	REGISTRATION/ USE OF INTERNAL SYSTEMS	FULL NAME, EMAIL (PERSONAL OR PROVIDED BY THE SCHOOL), ENROLLMENT NUMBER, LOGIN, AND PASSWORD.	EXECUTION OF CONTRACT OR PRELIMINARY PROCEDURES AT THE REQUEST OF THE DATA SUBJECT.	SPECIFIC AND HIGHLIGHTED CONSENT, GIVEN BY AT LEAST ONE OF THE PARENTS OR LEGAL GUARDIANS. CONTRACT EXECUTION
ERT	CONTINUITY OF SERVICE PROVISION	FULL NAME, EMAIL (PERSONAL OR PROVIDED BY THE SCHOOL), ENROLLMENT NUMBER, LOGIN, AND PASSWORD.	COMPLIANCE WITH LEGAL OR REGULATORY OBLIGATIONS.	COMPLIANCE WITH LEGAL OR REGULATORY OBLIGATIONS.

Source: Authors' own elaboration.

3. PROCESSING SENSITIVE DATA OF MINORS

LGPD states, in its Art. 5, II, that sensitive personal data is the one that deals with personal information on racial or ethnic origin, religious conviction, political opinion, membership

in a union or organization of a religious, philosophical, or political nature, health or sexual life, genetic or biometric data when linked to a natural person. There is a discussion about the accuracy or explanatory character of the mentioned article content. In this regard, it is necessary to bear in mind that the understanding of what represents sensitive data may vary from one country to another.

It is important to note that Art. 11 of the LGPD, which raises the hypotheses in which sensitive personal data can be processed,[14] states that its provisions apply to any treatment that *discloses* sensitive personal data and that may damage the data subject. In this context, there is objectively sensitive information, such as fingerprints and facial recognition, collected either in exams and in other means that can be inferred from the processing context. A person's image or voice may not present itself as sensitive data. But if it is used to identify race or ethnicity, it will have different circumstances.

Furthermore, sensitive personal information is the one whose processing may lead to discrimination against its data subject and is susceptible to stricter protection, in other words, the law should only authorize the processing of such data in indispensable situations, bringing the burden of proof of indispensability to the controller (CCGD, 2020, p. 22). It is always necessary to analyze specific cases; however, as a rule, the processing of biometric and genetic attributes should occur based on the regime for the processing of sensitive personal data (CCGD, 2020, p. 21).

In the following items, it will be analyzed the processing of sensitive personal data of adolescents for classes recording (synchronous teaching activities) and remote testing. It is argued that, for both purposes, the most adequate legal basis consists in obtaining the consent of the data subject, or of the person responsible for them, for certain purposes (Art. 11, I, of LGPD).

3.1 Use of Videoconferencing Platforms and Class Recording

The migration of education to remote teaching due to the pandemic has led many HEIs to make use of third-party service providers, such as Zoom, Google Meet, Microsoft Teams, among others, to continue synchronous class activities. It raises a number of concerns, especially from a privacy and data protection perspective. This movement of "platforming education" resulted in points of friction with the personal data protection regime, such as:

14 The hypotheses include: i) when the data subject/legal guardian consents, in a particular and prominent manner, for specific purposes; and ii) without the provision of consent, when it is essential for: a) compliance with a legal or regulatory obligation; b) execution of public policies provided for in laws or regulations; c) conducting studies by a body of research; d) regular exercise of rights; e) protection of life or physical safety of the owner or third party; f) health protection; and g) guarantee of fraud prevention and security of the data subject during the identification and authentication processes of registration in electronic systems.

the attribution of roles and responsibilities to the actors involved, the transparency of processing, and the possibility for data subjects to exercise their rights, in addition to the issue of international data transfer. The unclear definition of processing purposes, as well as the assignment of roles and responsibilities between the University and the platform, create a situation of detrimental opacity for the data subjects involved, including students and professors (ANGIOLINI *et al.*, 2020, p. 46-48).

Many of these platforms enable to record sessions. Regarding the personal data involved, filming students means that the recorded data may reveal (i) information about their racial or ethnic origin; (ii) attributes that may lead to their biometric identification; and (iii) expose statements that contain political opinion, membership in a union or organization of a religious, philosophical, or political nature, or either reference to information on health or sexual life.

In this regard, although HEIs hardly use the data of this type of recording (classes) for purposes such as ethnic-racial identification of the student, unlike what could happen in the college entrance examination panel that analyzes the admission of quota students, the great concern lies in inferences. Let's imagine that, in a class on party political organizations in Brazil, students start to express their positions. If the HEI reproduces it for other classes without the authorization of students, for example, this information will obviously be exposed, with inappropriate and discriminatory use of data, demanding accountability from HEI. Therefore, it is worth reflecting on whether this operation is necessary for processing data.

Therefore, the first question to be asked is: what is the purpose of data processing? Can this purpose be fulfilled in any other way? If there are less intrusive ways to accomplish it, the processing does not pass the test of the principle of necessity. It is noteworthy that the determination of the purpose and documentation of operations considering the risks associated with them must occur before the processing,[15] even because the National Data Protection Authority (ANPD) may determine that the controller must prepare an impact report on the protection of personal data, including sensitive ones, regarding its processing operations (Art. 37, of the LGPD).

If the purpose is service offering or continuity, there are other ways to do so. Possible options are, for instance, recording only the teacher in more expository approaches, as many applications are viable, such as Zoom, which features the speaker view mode, in such a way that only the teacher is filmed. Another option consists of editing videos and removing students' statements. In any case, it is interesting to point out that this option would generate the burden of due elimination for HEI.

15 The ICO GDPR Guide provides interesting observations on special category data (ICO, 2018).

It does not mean that the recording of classes with image and voice of students is prohibited, however, for providing educational services – or their continuity, the operation proves to be excessive.

During the pandemic, a question arose about how HEIs would prove that students were having access and availability to the content offered and that assessments were being carried out during the authorization period (as required by Art. 1 of MEC Ordinance No. 343, of March 17th, 2020). In this context, many HEIs started to consider recording the classes to prove, in case of inspection, that they were complying with the determination.

At this point, in an analogous sense, if the purpose is to prove compliance with a standard, other tools can be used to do so without collecting and processing sensitive data. Using the Zoom example again, the platform features, like many others (e.g.: Google Meet), a reporting tool, which shows who was responsible for opening the room, in which participants joined in, how long they stayed connected, what was the duration of the meeting (time stamp), in addition to the possibility of using the chat tool to register attendance, for example.

Therefore, to record images and voices of students, the most recommended legal basis is the consent of Art. 11, I, given by the data subject, or legal guardian in the case of children under 16 years of age. *But what if there is no consent?* If consent is not obtained, considering that recording, in this case, is not strictly necessary for the intended purpose, HEI needs to guarantee access to the content offered in other ways. As previously mentioned, editing may be used to delete a student's statement, for example.

A creative solution is to elaborate an image and voice usage term with a specific and highlighted clause for data protection. Mainly in the case of people over 16 years old and in small classes, the registration of consent could occur in the recording itself. After all, the LGPD does not require written consent. Furthermore, it is important to emphasize the impossibility of using the legitimate interest for operations carried out with sensitive data. This legal basis cannot be used to the detriment of the fundamental rights and freedoms of the data subject.

Regardless of the legal basis adopted for recording the image and voice of students, minors or not, the deletion of files is recommended at the end of the course, as well as that data subjects and their guardians have sufficient information about the technical and administrative measures adopted for data protection and storage, as well as disposal periods, in accordance with the pre-determined purposes of data processing. Furthermore, HEI must employ sufficient means to ensure the safety of this information (such as encryption, access control, and secure storage).

3.2 E-proctoring and RemoteTesting

Another current relevant issues are exams for admission to HEIs, such as college entrance examinations, which have a considerable number of applicants under 16 years of age. With the spread of COVID-19, testing in the online environment has also become a challenge,

including the question of how to prevent potential student fraud. Within this, concerns about ensuring the integrity and validity of this type of evidence started to rely on inspection systems (e-proctoring), which allow the monitoring of students in real-time (ANGIOLINI *et al.*, 2020, p. 64).

This type of exam emerged as an alternative for HEIs to continue their selection processes for admission, while also allowing people in different locations to be able to take exams without the need to leave their location. However, the functioning of these tools may depend on the collection and generation of personal data, so it is important to consider the context in which operations are performed and their purposes. This type of proof involves digital authenticators, in other words, biometric data, such as facial recognition and fingerprint collection. Would it be a prerogative of HEI to guarantee the veracity of the data?

Among the essential concerns about the protection of personal data, an important point is the data collected to *monitor* the candidate, such as the capture of photos, videos, audio, and screen activity during the exam. Furthermore, there is the fact that many electronic monitoring systems have shown difficulties in correctly recognizing black male and female students (ANGIOLINI *et al.*, 2020, p. 65).

Regarding data protection principles, particularly transparency, when collecting personal data from data subjects, it is necessary to inform them, in a clear and precise manner, as well as in an accessible and understandable language, about the processing that will be performed, including any sharing of information. It is also necessary to ensure that data processing takes place in accordance with the stated purposes and that only the strictly necessary personal data for the achievement of the determined processing purpose is indeed treated, avoiding the collection and use of excessive and unnecessary data.

There are several platform-specific services for pre-employment exams, so the processing linked to them may involve the collection of various personal data. The most common examples of it include (i) login and profile data (such as e-mail, first name, last name, username, password); (ii) candidate student contact details (such as telephone number, home address, etc.); (iii) time and duration of the test; (iv) audio, video and photo recording of the candidate; (v) answers to questions; (vi) transcription of candidates' responses in interviews; (vii) documents related to the selection process (resume, motivation letter, essay or other relevant documents); (viii) data from the electronic device to be used for the test (operating system, browser, processor, IP address, etc.); and (ix) activities and movements on the candidates' screen during the exam, as well as pages and applications used.

It is important to point out that data related to the documentation provided by the data subject to the selection process can be cross-checked with the information collected in the test, so that some platforms make the biometric capture at the time of registration, such as the EasyProctor. Video and audio monitoring is also common, in which the system transcribes the speech and sends alerts to the controller, gazes deviations, head movements to the opposite side of the screen, and detects face absences. Considering that HEIs have access

to all recordings and alerts and that they are responsible for contracting the services, they will be considered as controllers or co-controllers, depending on the specific case. Generally, the contractual instrument for this type of service, such as the one on the aforementioned platform, contains provisions for conducting audits, supervising tests, and carrying out remote monitorings.

Regarding remote evidence applications, a basis that could be claimed is the execution of a contract or preliminary procedures at the data subject request, as it would allow the processing of data to enforce the contract in which he or she is a party of and/or has an interest in the execution – in this case, the selection process. Similarly to consent, this basis could also be applied to the processing of sensitive personal data, by the provision of Art. 11, II, "d", of LGPD.

However, the greatest risk for using the legal basis of contract execution while collecting remote evidence is the possibility of claiming that not all personal data collected is essential or fundamental for the system functioning and test performance. This is because there may be differentiation in the purposes of data processing, some of which may, in fact, be essential for the technical implementation of the remote testing platform (such as information about the machine on which the candidate takes the test), while others would be handled to ensure a suitable process (such as monitoring of on-screen activities, as well as audio and video recordings) – a purpose that is relevant in the context of assessment or examination, but whose need can be further questioned whether it is possible to obtain the same contract performance through less invasive means.

The question about the possibility of using the basis of legitimate interest in remote testing arises when observing its choice for the same context in foreign universities, for example, the University of Tilburg, in the Netherlands. This university, for example, justifies the use of the legitimate interest basis (in the scope of the GDPR) arguing that the purpose of using remote assessment platforms is to maintain the quality of education and public value of diplomas issued by it, to avoid delays in studies, and to protect the health of its students and staff, among others. Furthermore, in certain cases, the university offers alternatives for students who do not wish to take the tests remotely.

However, even if the use of platforms is relevant to the institution's activities and there is a certain benefit to the candidate, there may be questions about the real need for all data processing related to assessments, especially those involving students monitoring.

It is also important to emphasize that, in cases in which the platforms have facial recognition features, other technologies that use biometric data or that in any other way handle sensitive personal data, the basis of legitimate interest cannot be applied, as it is not explained in the list of Art. 11, of the LGPD.

Although remote tests raise questions regarding the use of consent (Art. 11, I, of the LGPD) as a legal basis, it is argued that they are the most adequate foundations for this purpose. Evidently, there is difficulty in implementing a granular consent and acceptance for data

processing, especially related to the capture of photos, video, audio, etc., it would consist of a condition for participation in the test. In other words, using consent would not be possible to offer the candidate the option of agreeing to the processing of some data and rejecting others, not even proceeding with the examination.

However, we note that some of that data is effectively necessary for the technical implementation of the test system, such as the one related to the operating system and other information about the candidate's equipment. Other may be related to the justification of maintaining the suitability of the process and prevent fraud (e.g.: capturing of audio and image and monitoring of activities on the screen), ensuring the identity of individuals and preventing them from using consultation materials or methods which are not allowed. In part of the systems currently used, the verification of the candidate's identity or the suitability of their test environment depends on their constant sound and visual monitoring.

Thus, considering the characteristics of consent, especially the one that establishes that it must be free, conditioning remote tests to the acceptance of personal data processing in a "package", without the possibility of dividing it, seems, at first sight, invalid. However, the LGPD text itself allows such conditioning, as long as certain precautions are taken: Art. 9, paragraph 3, establishes that, in cases in which the processing of personal data is a condition for the supplying of a product, service, or the exercise of a right, the data subject must be prominently informed about this fact and about how they may exercise the rights provided for in Art. 18 of the law.

Although there is a risk in using consent as a legal basis for the processing of personal data in the context of remote testing, this basis can be used for the processing of common and sensitive personal data, as well as the ones for persons under 16 years of age. Furthermore, since such processing constitutes a condition for offering service, this fact must be duly informed to the data subject, along with information on how they may exercise their rights.

Conclusions

With this paper we sought to provide possible interpretations of the legal treatment regarding Art. 14 of the LGPD, along with related norms, looking for best practices and guaranteeing the protection of children and adolescents, while taking into account the issue of autonomy, especially considering the civil regime for the relatively incapable ones (people over 16 years old and under 18 years old). To support this contribution, we used international and foreign authorities references, in addition to the authors' experience in two years of research on strategies for compliance with personal data protection laws in Brazil and the implementation of procedures and development of materials for Higher Education. With this work, our proposal was also to design practical solutions for new difficulties faced by HEIs in Brazil, in addition to the need to adapt to the new law and international guidelines. The context of the pandemic accelerated the digitalization of education, and, with it, problems related to the

vulnerability of children and adolescents were added due to the protection of their personal data in digital medias and tools.

Following the example of European data protection regulations and valuing special and priority integral safeguard of children and adolescents, the LGPD brought stricter legal obligations to the controller responsible for handling personal data of such data subjects. The concern with this special category reflects the need to protect the developing person, considering their vulnerable status. In other words, children and adolescents will be less aware of the risks to which their fundamental rights and freedoms may be exposed.

The lack of clarity and detail on the LGPD's protection regime for minors raises a series of questions regarding the requirement of special consent (Art. 14, § 1). In this article, we sought to evidence this issue, exposing concrete situations that illustrate the changes that Brazil has been facing, especially in education.

Distance learning has been growing in recent decades and has become an important reference for the use of digital media for synchronous and asynchronous activities in teaching. In March 2020, there was a paradigm shift for HEIs with the use of the ERT. This change was accompanied by difficulties in its implementation, imposed by social isolation as a public policy. In addition, a solution given by the HEIs for the continuity of their admission selection processes was the use of remote testing, with sensitive data collection and candidate monitoring.

Regarding these contexts, we sought to propose an analysis of the most appropriate legal bases and the consequences of these choices for the processing of adolescents' data, as Art. 14, § 1, does not expressly mention teenagers when referring to special consent required for children. We acknowledge that it does not represent the only legal basis applicable to transactions carried out with data from minors; the special consent, however, it constitutes an important possibility for managing the parents or guardians and protecting the minor. In any case, the principles of need and transparency are essential for this choice process. Such protection should be prioritized by respecting the freedom and autonomy of the young person. There is no exact answer to every abstract hypothesis, but concrete circumstances must be analyzed within these parameters.

REFERENCES

ANGIOLINI, Chiara *et al*. Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of 'Platformised' Education. *Opinio Juris in Comparatione*: Studies in Comparative and National Law, [*s.l.*], v. 1, n. 1, p. 45-72, 2020. Available at: https://ssrn.com/abstract=3779238. Accessed on: July 7th, 2021.

ASSOCIAÇÃO BRASILEIRA DE ESTÁGIOS – ABRES. *Estatísticas*. 2020. Available at: https://abres.org.br/estatisticas/. Accessed on: Aug. 1st, 2021.

BIONI, Bruno Ricardo. *Proteção dos dados pessoais:* a função e os limites do consentimento. 2. ed. rev., atual. e reform. Rio de Janeiro: Forense, 2020.

BRASIL. Autoridade Nacional de Proteção de Dados. *Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.* Available at: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf. Accessed on: July 1st, 2021.

BRASIL. *Decreto Legislativo n. 6, de 20 de março de 2020*. Reconhece, para os fins do art. 65 da Lei Complementar n. 101, de 4 de maio de 2000, a ocorrência do estado de calamidade pública, nos termos da solicitação do Presidente da República encaminhada por meio da Mensagem n. 93, de 18 de março de 2020. 2020a. Available at: http://www.planalto.gov.br/ccivil_03/portaria/DLG6-2020.htm. Accessed on: Aug. 1st, 2021.

BRASIL. Governo Digital. *Lei Geral de Proteção de Dados (LGPD)*: guia de boas práticas para implementação na Administração Pública Federal. Apr. 2020b. Available at: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Accessed on: July 11th, 2021.

BRASIL. *Lei n. 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Accessed on: Aug. 1st, 2020.

BRASIL. Câmara dos Deputados. *Lei n. 10.406, de 10 de janeiro de 2002*. Institui o Código Civil. Available at: https://www2.camara.leg.br/legin/fed/lei/2002/lei-10406-10-janeiro-2002-432893-publicacaooriginal-1-pl.html. Accessed on: July 11th, 2021.

BRASIL. *Lei n. 8069, de 13 de julho de 1990*. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Available at: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Accessed on: August 1st, 2020.

BRASIL. Ministério da Educação. *Censo mostra que ingresso de alunos cresceu 8,5% em 2008*. Available at: http://portal.mec.gov.br/component/tags/tag/32123#:~:text=Em%202017%2C%20o%20aumento%20foi,queda%20no%20n%C3%BAmero%20de%20matr%C3%ADculas. Accessed on: Aug. 10th, 2021.

BRASIL. Ministério da Educação. *Perguntas frequentes sobre educação superior*. Available at: http://portal.mec.gov.br/sesu-secretaria-de-educacao-superior/perguntas-frequentes. Accessed on: Aug. 1st, 2021.

CASTIONI, Remi *et al*. Universidades federais na pandemia da covid-19: acesso discente à internet e ensino remoto emergencial. *Ensaio*: *Avaliação e Políticas Públicas em Educação* [online], v. 29, n. 111, p. 399-419, 2021. Available at: https://doi.org/10.1590/S0104-40362021002903108. Accessed on: May 29th, 2021.

DUBLIN CITY UNIVERSITY – DCU. *Data Protection Privacy Notice*: Recording of Lectures. Oct. 2nd, 2020. Available at: https://www.dcu.ie/sites/default/files/inline-files/1-dcu-privacy-notice-recording-of-lectures-v1-02.10.2020.pdf. Accessed on: Dec. 6th, 2020.

EUR-LEX. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016*. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Available at: https://eurlex.europa.eu/eli/reg/2016/679/oj?locale=pt. Accessed on: June 12th, 2020.

GUSSO, Hélder Lima *et al*. Ensino superior em tempos de pandemia: diretrizes à gestão universitária. *Educação & Sociedade*, Campinas, v. 41, e238957, 2020. Available at: https://doi.org/10.1590/ES.238957. Accessed on: May 29th, 2021.

INFORMATION COMMISSIONER'S OFFICE – ICO. *Guide to Data Protection*. Key data protection themes: children. United Kingdom. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/. Accessed on: Oct. 9th, 2023.

THE UNIVERSITY OF EDINBURGH – TUE. *Lecture Recording Policy*. Available at: https://www.ed.ac.uk/information-services/learning-technology/media-hopper-replay/help-and-support/frequently-asked-questions/lecture-recording-policy. Accessed on: Dec. 6th, 2020.

YANDRA, Barbara Fernanda Ferreira; SILVA; Amanda Cristina Alves; SANTOS, Jéssica Guedes. Lei Geral de Proteção de Dados e a tutela dos dados pessoais de crianças e adolescentes: a efetividade do consentimento dos pais ou responsáveis legais. *Internet & Sociedade*, [*s.l.*], v. 1, n. 1, p. 230-249, 2020. Available at: https://revista.internetlab.org.br/wp-content/uploads/2020/02/Lei-Geral-De-Protec%CC%A7a%CC%83o-De-Dados.pdf. Accessed on: Dec. 6th, 2020.

How to quote this article:

ZAPPELINI, Thaís Duarte; SCHIPPERS, Laurianne-Marie; SILVA, Alexandre Pacheco. Personal Data of Adolescents in Higher Education: The LGPD and the Use of Digital Media for Teaching Activities and Remote Testing. *Revista Direito GV*, São Paulo, v. 19, e2335, 2023. https://doi.org/10.1590/2317-6172202335

Thaís Duarte Zappelini

Post-Doctoral Fellow at the Lemann Center for Brazilian Studies (University of Illinois at Urbana-Champaign, USA). Ph.D. and Master in Political and Economic Law at Mackenzie Presbyterian University.

thaisdz@illinois.edu

Laurianne-Marie Schippers

Master's student in International Relations at the Institute of International Relations at the University of São Paulo (IRI – USP). Bachelor of Law from Getulio Vargas Foundation (FGV). Researcher at the Center for Education and Research on Innovation (CEPI – FGV DIREITO SP) at FGV.

laurianne.schippers@fgv.br

Alexandre Pacheco da Silva

Ph.D. in Scientific and Technological Policy from the Geosciences Institute of the State University of Campinas (Unicamp). Coordinator of the Researcher at the Center for Education and Research on Innovation (CEPI – FGV DIREITO SP) at Getulio Vargas Foundation (FGV). Professor of undergraduate and graduate programs at FGV DIREITO SP. Founder of the Laboratory for New Technology Companies (LENT), the Laboratory for Technological Development in Law (LabTEch) and the Innovation Laboratory (Inovalab). Coordinator of the Legal Hackers Study Group at FGV DIREITO SP.

alexandrepachecodasilva@gmail.com